



User's Guide

MGS3600-24F/XGS3600-26F/XGS3600-28F

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the switch using the web configurator.

Related Documents

- Command Line Interface (CLI) Reference Guide

The Command Reference Guide explains how to use the Command-Line Interface (CLI) and CLI commands to configure the switch.

- Web Configurator Online Help

The embedded Web Help contains descriptions of individual screens and supplementary information.

Note:

It is recommended you use the web configurator to configure the switch.

- Support Disc

Refer to the included CD for support documents.

Documentation Feedback

Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.

- Download Library

Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.

- Knowledge Base

If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.

- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

WARNING:

Warnings tell you about things that could harm you or your device.

Note:

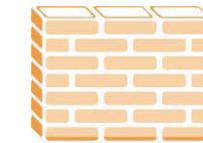
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The MGS3600-24F, XGS3600-26F and XGS3600-28F may be referred to as the “MGS3600-24F”, “XGS3600-26F”, “XGS3600-28F”, “switch”, the “device”, the “system” or the “product” in this User's Guide. Differentiation is made where needed.
- Product labels, screen names, field labels and field choices are all in bold font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the “enter” or “return” key on your keyboard.
- “Enter” means for you to type one or more characters and then press the [ENTER] key. “Select” or “choose” means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, Maintenance > Log > Log Setting means you first click Maintenance in the navigation panel, then the Log sub menu and finally the Log Setting tab to get to that screen.
- Units of measurement may denote the base-10 value or the base-2 value. For example, “k” for kilo may denote “1000” or “1024”, “M” for mega may denote “1000000” or “1048576” and so on.

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The switch icon is not an exact representation of your device.

The Switch	Computer	Notebook computer
		
Server	DSLAM	Firewall
		
Telephone	Switch	Router
		

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- For continued protection against risk of fire replace only with same type and rating of fuse.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



CONTENTS OVERVIEW

Front Matter

Front Matter

Introduction	1-2
Ways to Manage the Switch	1-3
Good Habits for Managing the Switch	1-4

Front Matter

Free Standing Installation	2-2
Rack-Mounted Installation	2-4
Rack-mounted Installation Requirements	2-4
Precautions	2-4
Attaching the Mounting Brackets to the Switch	2-5
Mounting the Switch on a Rack	2-6

Front Matter

Front Panel Connections	3-2
Dual Personality Interfaces	3-5
1000Base-T Ports	3-6
Default Ethernet Settings	3-6
Mini-GBIC Slots.....	3-7
Transceiver Installation	3-8
Transceiver Removal	3-9
Power Connectors.....	3-10
Console Port	3-12
LEDs	3-13

Front Matter

Overview.....	4-2
Traffic Overview.....	4-3
Status: Port Details	4-5

Front Matter

Overview.....	5-2
---------------	-----

What You Can Do	5-3
System Information.....	5-4
General Setup.....	5-7
VLANs.....	5-10
IP Setup	5-12
Management IP Addresses.....	5-12
Port Configuration.....	5-15

Front Matter

Front Matter

System Configuration	6-5
System Information.....	6-6
Information	6-6
Configuration.....	6-9
CPU Load.....	6-10
Time.....	6-11
Manual	6-11

NTP	6-13
Account	6-14
Users	6-14
Privilege Level	6-16
IP	6-17
IPv4	6-17
IPv6	6-19
SYSLOG	6-20
Configuration	6-20
Log	6-21
Detailed Log	6-22
SNMP	6-23
System	6-23
Communities	6-24
Users	6-25
Groups	6-27
Views	6-28

Access.....	6-29
Trap.....	6-31

Front Matter

Configuration	7-2
Port	7-3
Configuration.....	7-3
Port Description.....	7-5
Traffic Overview	7-6
Detailed Statistics.....	7-7
QoS Statistics.....	7-9
SFP Information	7-10
ACL.....	7-12
Ports.....	7-12
Rate Limiters.....	7-14
Access Control List	7-15
ACL Status.....	7-21
Aggregation	7-23

Static Trunk.....	7-23
LACP.....	7-25
Spanning Tree	7-29
Bridge Settings.....	7-30
MSTI Mapping.....	7-32
MSTI Priorities.....	7-33
CIST Ports.....	7-34
MSTI Ports	7-36
Bridge Status.....	7-37
Port Status	7-39
Port Statistics	7-40
MRSTP	7-41
Instances.....	7-41
Port Configuration	7-44
Port Status	7-46
IGMP and MLD Snooping.....	7-48
Basic Configuration	7-48

VLAN Configuration	7-50
Port Group Filtering.....	7-52
Status	7-53
Group Information	7-55
IPv4 and IPv6 SSM Information	7-56
MVR.....	7-57
Configuration.....	7-57
Groups Information	7-59
Statistics.....	7-60
LLDP	7-61
LLDP Configuration.....	7-61
LLDP Neighbors.....	7-64
LLDP MED Configuration.....	7-65
LLDP MED Neighbors.....	7-71
Port Statistics	7-74
Configuration.....	7-76
Dynamic MAC Table	7-78

VLAN	7-79
VLAN Membership	7-79
Ports	7-80
Switch Status	7-82
Port Status	7-83
Private VLANs	7-84
MAC-Based VLAN	7-86
Protocol-Based VLAN	7-88
GARP and MRP	7-90
Configuration	7-90
Statistics	7-92
GVRP and MVRP	7-93
Configuration	7-93
Statistics	7-95
QoS	7-96
Port Classification	7-96
Port Policing	7-99

Queue Policing.....	7-101
Port Scheduler and Port Shaping.....	7-102
Port Tag Remarking.....	7-104
Port DSCP.....	7-106
DSCP Based QoS.....	7-107
DSCP Translation	7-108
DSCP Classification	7-109
QoS Control List.....	7-110
QCL Status.....	7-114
WRED	7-116
sFlow Agent.....	7-118
Collector.....	7-118
Sampler.....	7-120
Mirroring.....	7-121
Trap Event Severity	7-122
SMTP Configuration	7-123
802.3ah OAM.....	7-124

Port Config	7-124
Event Config.....	7-126
Port Status	7-128
Link Events.....	7-130
Statistics.....	7-133
Ethernet OAM	7-135
EPS.....	7-137
EPRS	7-139

Security

Security.....	8-2
IP Source Guard	8-3
Configuration.....	8-3
Static Table	8-4
Dynamic Table	8-5
ARP Inspection	8-6
Configuration.....	8-6
Static Table	8-7

Dynamic Table	8-8
DHCP Snooping	8-9
Configuration.....	8-9
Statistics.....	8-10
DHCP Relay	8-12
Configuration.....	8-12
Statistics.....	8-13
NAS	8-15
Configuration.....	8-15
Switch Status	8-22
Port Status	8-23
AAA.....	8-25
Configuration.....	8-25
RADIUS Overview.....	8-28
RADIUS Details.....	8-29
Port Security	8-33
Limit Control.....	8-33

Switch Status	8-36
Port Status	8-38
Access Management	8-40
Configuration.....	8-40
Statistics.....	8-42
SSH	8-43
HTTPS	8-44
AUTH Method	8-45

Maintenance

Restart Device	9-2
Firmware.....	9-3
Firmware Upgrade	9-3
Firmware Selection	9-4
Save/Restore	9-5
Factory Defaults.....	9-5
Save Start	9-6
Save User	9-7

Restore User.....	9-8
Export/Import	9-9
Export Config	9-9
Import Config.....	9-10
Diagnostics	9-11
Ping.....	9-11
Ping6.....	9-12

Front Matter

Front Matter

Power, Hardware Connections and LEDs	10-3
Switch Access and Login.....	10-4
Switch Configuration.....	10-6

Front Matter

Hardware Specifications	11-2
Firmware Specifications.....	11-7

EMI/Safety Specifications	11-19
---------------------------------	-------

Front Matter

Glossary of Web Based Management	A-1
Common Services	B-1
Legal Information	C-1

TABLE OF CONTENTS

About This User's Guide

Intended Audience	ii
Related Documents	ii
Documentation Feedback	ii
Customer Support	iii

Document Conventions

Safety Warnings

Front Matter

Front Matter

Introduction	1-2
--------------------	-----

Ways to Manage the Switch	1-3
Good Habits for Managing the Switch	1-4

Front Matter

Free Standing Installation	2-2
Rack-Mounted Installation	2-4
Rack-mounted Installation Requirements	2-4
Precautions	2-4
Attaching the Mounting Brackets to the Switch.....	2-5
Mounting the Switch on a Rack.....	2-6

Front Matter

Front Panel Connections	3-2
Dual Personality Interfaces	3-5
1000Base-T Ports	3-6
Default Ethernet Settings	3-6
Mini-GBIC Slots.....	3-7
Transceiver Installation	3-8

Transceiver Removal	3-9
Power Connectors.....	3-10
AC Power Connection	3-10
DC Power Connection	3-11
Console Port	3-12
LEDs	3-13

Front Matter

Overview.....	4-2
Traffic Overview.....	4-3
Status: Port Details	4-5

Front Matter

Overview.....	5-2
What You Can Do	5-3
System Information.....	5-4
General Setup.....	5-7
VLANs.....	5-10

IP Setup	5-12
Management IP Addresses	5-12
Port Configuration	5-15

Front Matter

Front Matter

System Configuration	6-5
System Information	6-6
Information	6-6
Parameter description	6-6
Configuration	6-9
Parameter description	6-9
CPU Load	6-10
Time	6-11
Manual	6-11
Parameter description	6-11
NTP	6-13

Parameter description.....	6-13
Account.....	6-14
Users.....	6-14
Parameter description.....	6-14
Privilege Level.....	6-16
Parameter description.....	6-16
IP	6-17
IPv4.....	6-17
Parameter description.....	6-17
IPv6.....	6-19
Parameter description.....	6-19
SYSLOG	6-20
Configuration.....	6-20
Parameter description.....	6-20
Log	6-21
Parameter description.....	6-21
Detailed Log	6-22

Parameter description.....	6-22
SNMP	6-23
System	6-23
Parameter description.....	6-23
Communities	6-24
Parameter description.....	6-24
Users.....	6-25
Parameter description.....	6-25
Groups	6-27
Parameter description.....	6-27
Views.....	6-28
Parameter description.....	6-28
Access.....	6-29
Parameter description.....	6-29
Trap.....	6-31
Front Matter	
Configuration	7-2

Port	7-3
Configuration.....	7-3
Parameter description.....	7-3
Port Description.....	7-5
Parameter description.....	7-5
Traffic Overview	7-6
Parameter description.....	7-6
Detailed Statistics.....	7-7
Parameter description.....	7-7
QoS Statistics.....	7-9
Parameter description.....	7-9
SFP Information	7-10
Parameter description.....	7-10
ACL.....	7-12
Ports.....	7-12
Parameter description.....	7-12
Rate Limiters.....	7-14

Parameter description.....	7-14
Access Control List	7-15
Parameter description.....	7-15
ACE Conditions.....	7-15
ACE Actions	7-20
ACL Status	7-21
Parameter description.....	7-21
Aggregation	7-23
Static Trunk.....	7-23
Parameter description.....	7-23
Aggregation Mode Configuration	7-23
Aggregation Group Configuration	7-24
LACP.....	7-25
Configuration	7-25
Parameter description	7-25
System Status.....	7-26
Parameter description.....	7-26

Port Status	7-27
Parameter description.....	7-27
Port Statistics	7-28
Parameter description.....	7-28
Spanning Tree	7-29
Bridge Settings.....	7-30
Parameter description.....	7-30
Basic Settings	7-30
Advanced Settings	7-31
MSTI Mapping.....	7-32
Parameter description.....	7-32
Configuration Identification.....	7-32
MSTI Mapping	7-32
MSTI Priorities.....	7-33
Parameter description.....	7-33
CIST Ports.....	7-34
Parameter description.....	7-34

MSTI Ports	7-36
Parameter description.....	7-36
Bridge Status.....	7-37
Parameter description.....	7-37
Port Status	7-39
Parameter description.....	7-39
Port Statistics	7-40
Parameter description.....	7-40
MRSTP	7-41
Instances.....	7-41
Parameter description.....	7-41
MRSTP Instance Configuration.....	7-41
MRSTP Instance Status.....	7-42
Port Configuration	7-44
Parameter description.....	7-44
Port Status	7-46
Parameter description.....	7-46

IGMP and MLD Snooping	7-48
Basic Configuration	7-48
Parameter description.....	7-48
IGMP or MLD Snooping Configuration.....	7-48
Port Related Configuration.....	7-49
VLAN Configuration	7-50
Parameter description.....	7-50
Port Group Filtering.....	7-52
Parameter description.....	7-52
Status	7-53
Parameter description.....	7-53
Group Information	7-55
Parameter description.....	7-55
IPv4 and IPv6 SSM Information.....	7-56
Parameter description.....	7-56
MVR	7-57
Configuration.....	7-57

Parameter description.....	7-57
Groups Information	7-59
Parameter description.....	7-59
Statistics.....	7-60
Parameter description.....	7-60
LLDP	7-61
LLDP Configuration.....	7-61
Parameter description.....	7-61
LLDP Neighbors.....	7-64
Parameter description.....	7-64
LLDP MED Configuration.....	7-65
Parameter description.....	7-65
Fast Start Repeat Count	7-65
Coordinates Location	7-66
Civic Address Location.....	7-66
Policies.....	7-68
Policy Port Configuration.....	7-70

LLDP MED Neighbors.....	7-71
Parameter description.....	7-71
Port Statistics	7-74
Parameter description.....	7-74
Global Counters	7-74
Local Counters	7-74
Configuration.....	7-76
Parameter description.....	7-76
Aging Configuration.....	7-76
MAC Table Learning	7-76
Static MAC Table Configuration.....	7-77
Dynamic MAC Table	7-78
Parameter description.....	7-78
VLAN	7-79
VLAN Membership	7-79
Parameter description.....	7-79
Ports.....	7-80

Parameter description.....	7-80
Switch Status	7-82
Parameter description.....	7-82
Port Status	7-83
Parameter description.....	7-83
Private VLANs.....	7-84
Private VLANs Membership.....	7-84
Parameter description.....	7-84
Port Isolation.....	7-84
Parameter description.....	7-85
MAC-Based VLAN	7-86
Configuration	7-86
Parameter description.....	7-86
Status.....	7-87
Parameter description.....	7-87
Protocol-Based VLAN	7-88
Protocol to Group.....	7-88

Parameter description.....	7-88
Group to VLAN	7-89
Parameter description.....	7-89
GARP and MRP.....	7-90
Configuration.....	7-90
Parameter description.....	7-90
Statistics.....	7-92
Parameter description.....	7-92
GVRP and MVRP	7-93
Configuration.....	7-93
Parameter description.....	7-93
Global Configuration	7-93
Port Configuration	7-93
Statistics.....	7-95
Parameter description.....	7-95
QoS.....	7-96
Port Classification	7-96

Parameter description.....	7-96
Port Classification page	7-96
QoS Ingress Port Tag Classification page	7-97
Port Policing	7-99
Parameter description.....	7-99
Queue Policing.....	7-101
Parameter description.....	7-101
Port Scheduler and Port Shaping.....	7-102
Parameter description.....	7-102
Queue Shaper.....	7-102
Queue Scheduler	7-102
Port Shaper	7-103
Port Tag Remarking	7-104
Parameter description.....	7-104
PCP/DEI Configuration	7-104
DP level Configuration	7-104
(QoS class, DP level) to (PCP, DEI) Mapping	7-105

Port DSCP.....	7-106
Parameter description.....	7-106
DSCP Based QoS.....	7-107
Parameter description.....	7-107
DSCP Translation	7-108
Parameter description.....	7-108
DSCP Classification	7-109
Parameter description.....	7-109
QoS Control List.....	7-110
Parameter description.....	7-110
QCE Conditions	7-110
QCE Actions.....	7-113
QCL Status.....	7-114
Parameter description.....	7-114
WRED	7-116
Parameter description.....	7-117
sFlow Agent	7-118

Collector	7-118
Parameter description.....	7-118
Sampler.....	7-120
Parameter description.....	7-120
Mirroring.....	7-121
Parameter description.....	7-121
Trap Event Severity	7-122
Parameter description.....	7-122
SMTP Configuration	7-123
Parameter description.....	7-123
802.3ah OAM.....	7-124
Port Config	7-124
Parameter description.....	7-124
Event Config.....	7-126
Parameter description.....	7-126
Port Status	7-128
Parameter description.....	7-128

Link Events.....	7-130
Parameter description.....	7-130
Local and Remote Frame Error Status	7-130
Local and Remote Frame Period Status	7-130
Local and Remote Symbol Period Status	7-131
Local and Remote Event Seconds Summary Status	7-132
Statistics.....	7-133
Parameter description.....	7-133
Ethernet OAM	7-135
Parameter description.....	7-135
EPS.....	7-137
Parameter description.....	7-137
EPRS	7-139
Parameter description.....	7-139
Security	
Security.....	8-2
IP Source Guard	8-3

Configuration.....	8-3
Parameter description.....	8-3
IP Source Guard Configuration	8-3
Port Mode Configuration	8-3
Static Table	8-4
Parameter description.....	8-4
Dynamic Table	8-5
Parameter description.....	8-5
ARP Inspection	8-6
Configuration.....	8-6
Parameter description.....	8-6
ARP Inspection Configuration	8-6
Port Mode Configuration	8-6
Static Table	8-7
Parameter description.....	8-7
Dynamic Table	8-8
Parameter description.....	8-8

DHCP Snooping	8-9
Configuration.....	8-9
Parameter description.....	8-9
DHCP Snooping Configuration	8-9
Port Mode Configuration	8-9
Statistics.....	8-10
Parameter description.....	8-10
DHCP Relay	8-12
Configuration.....	8-12
Parameter description.....	8-12
Statistics.....	8-13
Parameter description.....	8-13
Server Statistics	8-13
Client Statistics.....	8-14
NAS	8-15
Configuration.....	8-15
Parameter description.....	8-15

System Configuration	8-15
Port Mode Configuration	8-17
Switch Status	8-22
Parameter description.....	8-22
Port Status	8-23
Parameter description.....	8-23
Port State	8-23
Port Counters	8-23
Attached MAC Addresses	8-24
AAA.....	8-25
Configuration.....	8-25
Parameter description.....	8-25
Common Server Configuration.....	8-25
TACACS+ Authorization and Accounting Configuration	8-26
RADIUS Authentication Server Configuration.....	8-26
RADIUS Accounting Server Configuration.....	8-26
TACACS+ Authentication Server Configuration.....	8-27

RADIUS Overview.....	8-28
Parameter description.....	8-28
RADIUS Details.....	8-29
Parameter description.....	8-29
RADIUS Authentication Statistics	8-29
RADIUS Accounting Statistics	8-31
Port Security	8-33
Limit Control.....	8-33
Parameter description.....	8-33
System Configuration.....	8-33
Port Configuration	8-34
Switch Status	8-36
Parameter description.....	8-36
User Module Legend.....	8-36
Port Status	8-36
Port Status	8-38
Parameter description.....	8-38

Access Management	8-40
Configuration.....	8-40
Parameter description.....	8-40
Statistics.....	8-42
Parameter description.....	8-42
SSH	8-43
Parameter description.....	8-43
HTTPS	8-44
Parameter description.....	8-44
AUTH Method	8-45
Parameter description.....	8-45

Maintenance

Restart Device	9-2
Firmware.....	9-3
Firmware Upgrade	9-3
Firmware Selection	9-4
Parameter description.....	9-4

Save/Restore	9-5
Factory Defaults	9-5
Save Start	9-6
Save User	9-7
Restore User	9-8
Export/Import	9-9
Export Config	9-9
Import Config	9-10
Diagnostics	9-11
Ping	9-11
Parameter description	9-11
Ping6	9-12
Parameter description	9-12

Front Matter

Front Matter

Power, Hardware Connections and LEDs	10-3
--	------

Switch Access and Login.....	10-4
Switch Configuration.....	10-6
Front Matter	
<hr/>	
Hardware Specifications	11-2
Key Features	11-2
Interface.....	11-3
LED Indicators	11-4
General	11-5
Firmware Specifications.....	11-7
Port Control.....	11-7
QoS.....	11-8
L2 Switching	11-9
Security and Synchronization	11-12
OAM.....	11-13
Robustness and Power Saving.....	11-14
Management.....	11-15
MIBs.....	11-16

EMI/Safety Specifications	11-19
---------------------------------	-------

Front Matter

Appendix A

Glossary of Web Based Management	A-1
A	A-1
C	A-3
D	A-4
E	A-6
F	A-7
H	A-8
I	A-9
L	A-11
M	A-12
N	A-14
O	A-15
P	A-16

Q	A-18
R	A-19
S	A-20
T	A-23
U	A-25
V	A-26

Appendix B

Common Services	B-1
-----------------------	-----

Appendix C

Legal Information	C-1
-------------------------	-----

Copyright	C-1
-----------------	-----

Disclaimer	C-1
------------------	-----

Trademarks	C-1
------------------	-----

Certifications	C-1
----------------------	-----

Federal Communications Commission (FCC) Interference Statement	C-1
--	-----

FCC Warning	C-2
-------------------	-----

CE Mark Warning:.....	C-2
Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:.....	C-2
Notices	C-2
Viewing Certifications.....	C-3
ZyXEL Limited Warranty	C-3
Note.....	C-3
Registration	C-3

Part I: Front Matter

Front Matter

Chapter 1

1.1 Introduction

This chapter introduces the main features and applications of the switch. The switch comes in the following models:

- MGS3600-24F 20-port GbE Fiber L2 Switch with Four GbE Combo Ports
- XGS3600-26F 20-port GbE Fiber L2 Switch with Four GbE Combo Ports and Two 10G Fiber Ports
- XGS3600-28F 20-port GbE Fiber L2 Switch with Four GbE Combo Ports and Four 10G Fiber Ports

The switch is a layer-2 standalone Ethernet switch with additional layer-2, layer-3, and layer-4 features suitable for Ethernets. With its built-in web configurator, managing and configuring the switch is easy. In addition, the switch can also be managed via Telnet, any terminal emulator program on the console port, or third-party SNMP management.

See “Firmware Specifications” on page 11-7 for a full list of software features available on the switch.

1.2 Ways to Manage the Switch

Use any of the following methods to manage the switch.

- Web Configurator. This is recommended for everyday management of the switch using a (supported) web browser.
- Command Line Interface. Line commands offer an alternative to the Web Configurator and may be necessary to configure advanced features. See the CLI Reference Guide.
- SNMP. The device can be monitored and/or managed by an SNMP manager. See “SNMP” on page 6-23.

1.3 Good Habits for Managing the Switch

Do the following things regularly to make the switch more secure and to manage the switch more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it).

Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the switch to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the switch. You could simply restore your last configuration.

Front Matter

Chapter 2

2.1 Free Standing Installation

This chapter shows you how to install and connect the switch.

1. Make sure the switch is clean and dry.
2. Set the switch on a smooth, level surface strong enough to support the weight of the switch and the connected cables. Make sure there is a power outlet nearby.
3. Make sure there is enough clearance around the switch to allow air circulation and the attachment of cables and the power cord.
4. Remove the adhesive backing from the rubber feet.
5. Attach the rubber feet to each corner on the bottom of the switch. These rubber feet help protect the switch from shock or vibration and ensure space between devices when stacking.

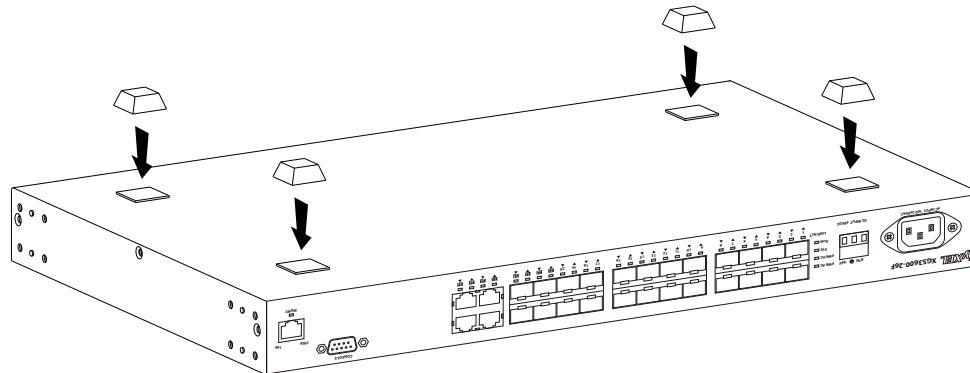


Figure 2-1. MGS3600-24F/XGS3600-26F/XGS3600-28F Attaching Rubber Feet

Note:

Do NOT block the ventilation holes. Leave space between devices when stacking.

Note:

For proper ventilation, allow at least 4 inches (10 cm) of clearance at the front and 3.4 inches (8 cm) at the back of the switch. This is especially important for enclosed rack installations.

2.2 Rack-Mounted Installation

This section lists the rack mounting requirements and precautions and describes the installation steps.

2.2.1 Rack-mounted Installation Requirements

- Two mounting brackets.
- Eight M3 flat head screws and a #2 Phillips screwdriver.
- Four M5 flat head screws and a #2 Phillips screwdriver.

WARNING:

Failure to use the proper screws may damage the unit.

2.2.1.1 Precautions

- Make sure the rack will safely support the combined weight of all the equipment it contains.
- Make sure the position of the switch does not make the rack unstable or top heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

2.2.2 Attaching the Mounting Brackets to the Switch

1. Position a mounting bracket on one side of the switch, lining up the four screw holes on the bracket with the screw holes on the side of the switch.

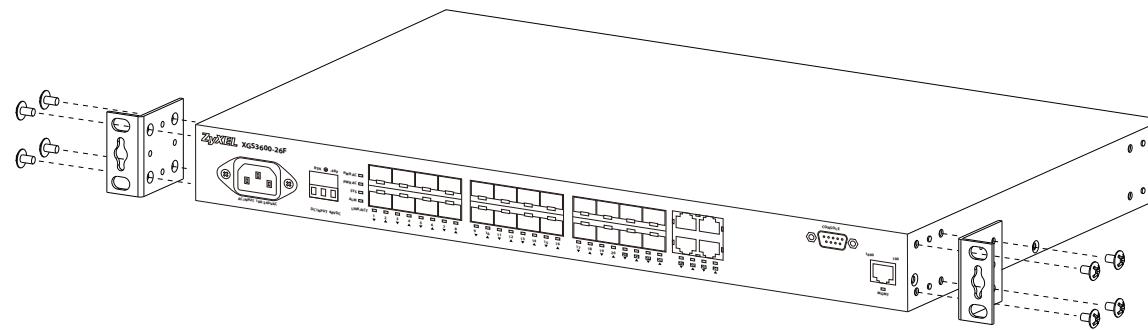


Figure 2-2. MGS3600-24F/XGS3600-26F/XGS3600-28F Attaching the Mounting Brackets

2. Using a #2 Phillips screwdriver, install the M3 flat head screws through the mounting bracket holes into the switch.
3. Repeat steps 1 and 2 to install the second mounting bracket on the other side of the switch.
4. You may now mount the switch on a rack. Proceed to the next section.

2.2.3 Mounting the Switch on a Rack

1. Position a mounting bracket (that is already attached to the switch) on one side of the rack, lining up the two screw holes on the bracket with the screw holes on the side of the rack.

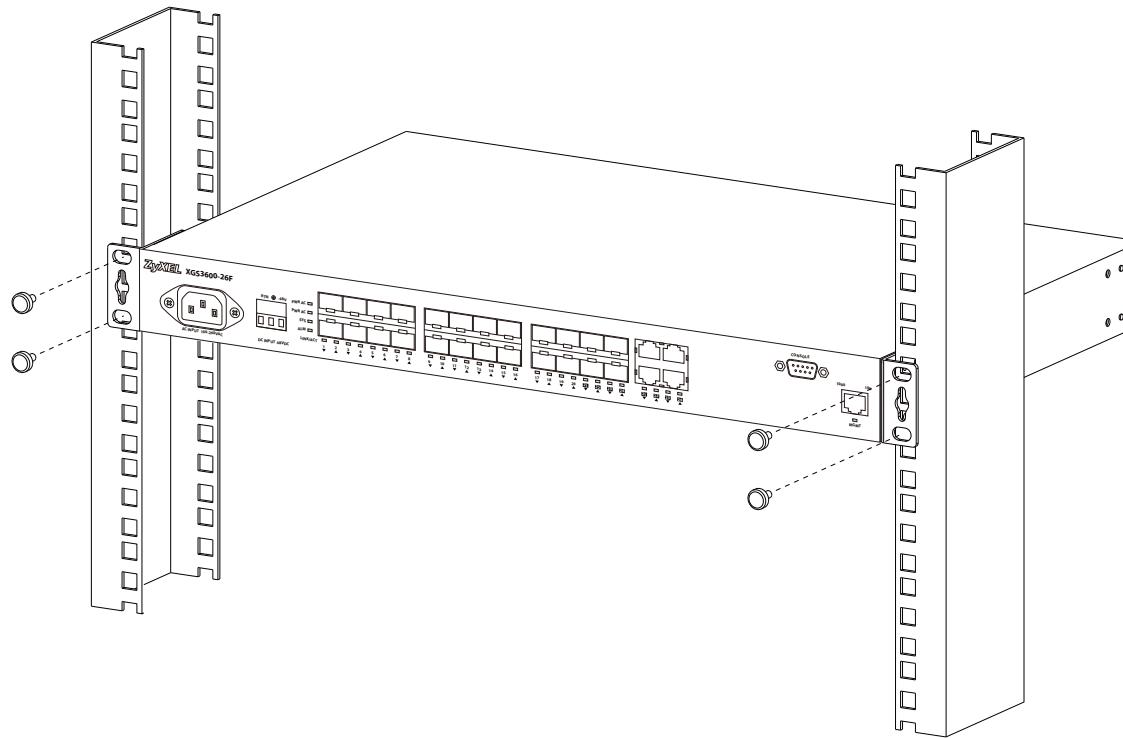


Figure 2-3. MGS3600-24F/XGS3600-26F/XGS3600-28F Mounting the Switch on a Rack

2. Using a #2 Phillips screwdriver, install the M5 flat head screws through the mounting bracket holes into the rack.
3. Repeat steps 1 and 2 to attach the second mounting bracket on the other side of the rack.

Front Matter

Chapter 3

3.1 Front Panel Connections

This chapter describes the front panel of the switch.

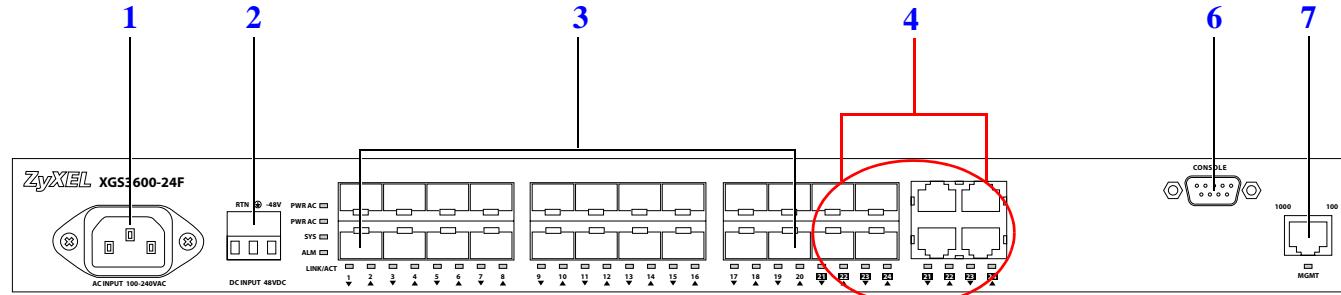


Figure 3-1. MGS3600-24F Front Panel

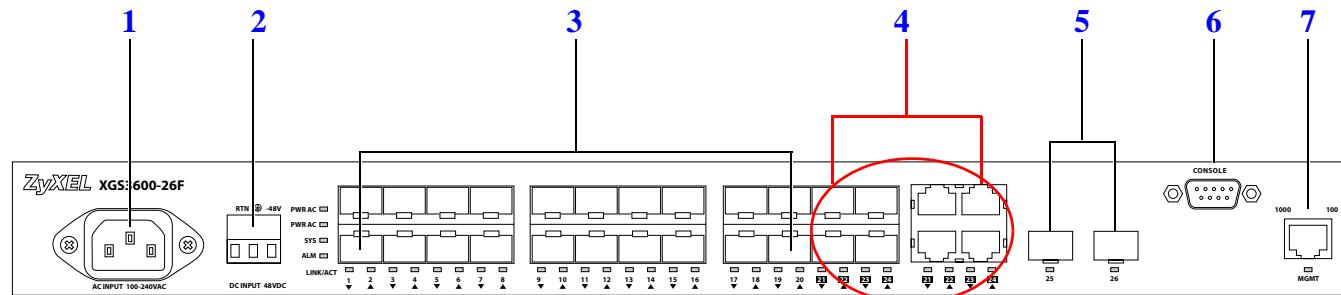


Figure 3-2. XGS3600-26F Front Panel

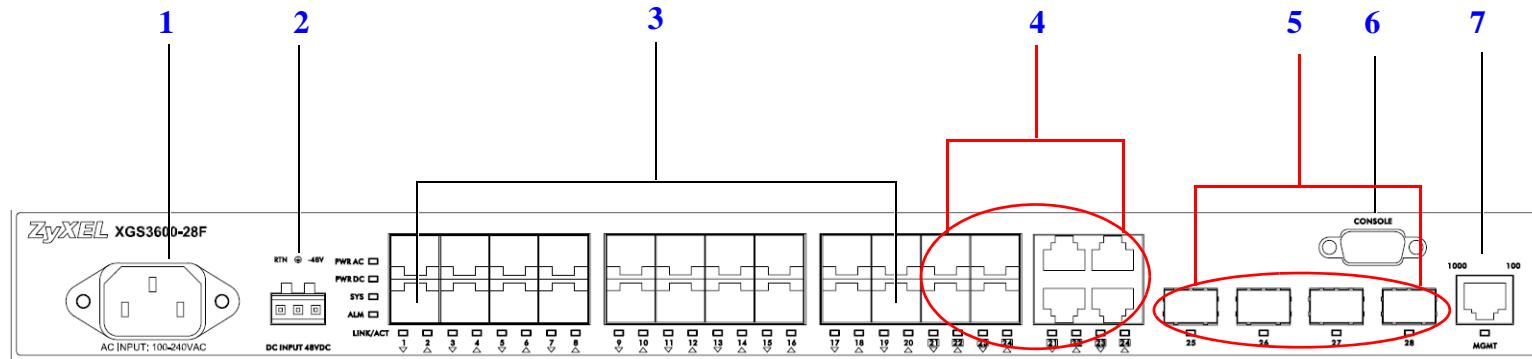


Figure 3-3. XGS3600-28F Front Panel

Table 3-1: Front Panel Connections

	CONNECTOR	DESCRIPTION
1	AC Power Socket	Connect this to AC power from the mains electricity grid.
2	DC Backup Power Supply 3-pin terminal block	Connect 48 V DC backup power to here.
3	SFP Subscriber Ports (20 x 100/1000 Mbps)	Connect these ports to a subscriber's computer.
4	SFP/RJ-45 Dual Personality Interfaces (4)	Connect these interfaces to local servers, routers or switches. Each interface consists of a pair of ports — one SFP (100/1000 Mb) port and one RJ-45 (10/100/1000Base-T) port. Only one port may be active at a time.

Table 3-1: Front Panel Connections

	CONNECTOR	DESCRIPTION
5	SFP+ Uplink Ports (2 x 1/10 Gbps)	Connect these ports to the distribution layer of the network (XGS3600-28F only).
6	RS-232 Management Port	Connect this port to an RS-232 interface to configure the switch using the command line interface (CLI).
7	RJ-45 Management Port (10/100/1000 Mbps)	Connect this Ethernet port to the out-of-band remote management network.

3.1.1 Dual Personality Interfaces

There are four Dual Personality interfaces, comprising four 1000Base-T and four mini-GBIC combo ports. For each interface you can connect either to the 1000Base-T port or the mini-GBIC port. The mini-GBIC ports have priority over the 1000Base-T ports. This means that if a mini-GBIC port and the corresponding 1000Base-T port are connected at the same time, the 1000Base-T port will be disabled.

3.1.2 1000Base-T Ports

The switch has 24 (26 for the XGS3600-26F only) 1000Base-T mini-GBIC Ethernet ports. In 100/1000 Mbps Gigabit Ethernet, the speed can be 100 Mbps or 1000 Mbps. The duplex mode can be both half or full duplex at 100 Mbps and full duplex only at 1000 Mbps.

An auto-negotiating port can detect and adjust to the optimum Ethernet speed (100/1000 Mbps) and duplex mode (full duplex or half duplex) of the connected device.

An auto-crossover (auto-MDI/MDI-X) port automatically works with a straight through or crossover Ethernet cable.

3.1.2.1 Default Ethernet Settings

The factory default negotiation settings for the Ethernet ports on the switch are:

- Speed: Auto
- Duplex: Auto
- Flow control: Off

3.1.3 Mini-GBIC Slots

These are 24 (26 for the XGS3600-26F only) slots for Small Form-Factor Pluggable (SFP) transceivers. A transceiver is a single unit that houses a transmitter and a receiver. Use a transceiver to connect a fiber-optic cable to the switch. The switch does not come with transceivers. You must use transceivers that comply with the Small Form-Factor Pluggable (SFP) Transceiver MultiSource Agreement (MSA). See the SFF committee's INF-8074i specification Rev 1.0 for details.

You can change transceivers while the switch is operating. You can use different transceivers to connect to Ethernet switches with different types of fiber-optic connectors.

- Type: SFP connection interface
- Connection speed: 1 Gigabit per second (Gbps) or 10 Gbps for the 2 uplink ports on the XGS3600-26F only

WARNING:

To avoid possible eye injury, do not look into an operating fiber optic module's connectors.

3.1.3.2 Transceiver Installation

Use the following steps to install a mini GBIC transceiver (SFP or XFP module).

1. Insert the transceiver into the slot with the exposed section of PCB board facing down.

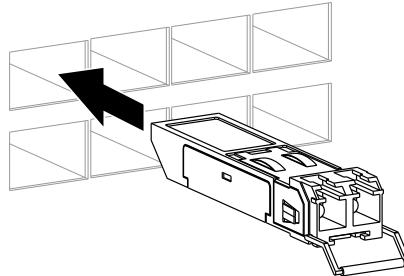


Figure 3-4. Transceiver Installation Example

2. Press the transceiver firmly until it clicks into place.
3. The switch automatically detects the installed transceiver. Check the LEDs to verify that it is functioning properly.

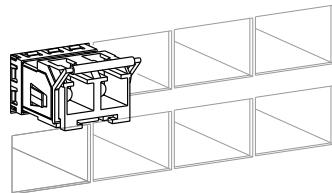


Figure 3-5. Installed Transceiver

3.1.3.3 Transceiver Removal

Use the following steps to remove a mini GBIC transceiver (SFP module).

1. Open the transceiver's latch (styles vary).

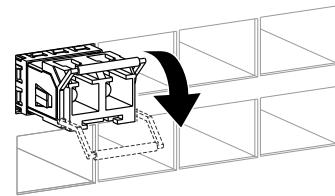


Figure 3-6. Opening the Transceiver's Latch Example

2. Pull the transceiver out of the slot.

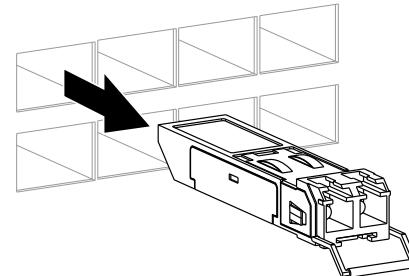


Figure 3-7. Transceiver Removal Example

3.1.4 Power Connectors

Use the following procedures to connect the switch to a power source after you have installed it.

WARNING:

Make sure you are using the correct power source as shown on the panel and that no objects obstruct the airflow of the fans. Use only power wires of the required diameter for connecting the switch to a power supply.

AC Power Connection

1. Connect the female end of the power cord to the power socket of your switch.
2. Connect the other end of the cord to a power outlet.

DC Power Connection

The switch uses a single ETB series terminal block plug with four pins which allows you to connect up to two separate power supplies. If one power supply fails the system can operate on the remaining power supply. Use two wires to connect to a single terminal pair, one wire for the positive terminal and one wire for the negative terminal.

Note:

When installing the power wire, push it wire firmly into the terminal as deep as possible and make sure that no exposed (bare) wire can be seen or touched.

WARNING:

Exposed power wire is dangerous. Use extreme care when connecting a DC power source to the device.

To connect a power supply:

1. Use a screwdriver to loosen the terminal block captive screws.
2. Connect one end of a power wire to the switch's RTN (return) pin and tighten the captive screw.
3. Connect the other end of the power wire to the positive terminal on the power supply.
4. Connect one end of a power wire to the switch's -48V (input) pin and tighten the captive screw.
5. Connect the other end of the power wire to the negative terminal on the power supply.
6. Insert the terminal block plug in the switch's terminal block header.

3.1.5 Console Port

For local management, you can use a computer with terminal emulation software configured to the following parameters:

- VT100 terminal emulation
- 115200 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

Connect the male 9-pin end of the RS-232 console cable to the console port of the switch. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

3.1.6 LEDs

The following table describes the LEDs.

Table 3-2: LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR DC	Green	On	The backup power supply is connected and active.
		Off	The backup power supply is not ready or not active.
PWR AC	Green	On	The system is turned on.
		Off	The system is off.
SYS	Green	Blinking	The system is rebooting and performing self-diagnostic tests.
		On	The system is on and functioning properly.
		Off	The power is off or the system is not ready/ malfunctioning.
ALM	Red	On	There is a hardware failure.
		Off	The system is functioning normally.
RJ-45 Dual Personality 1000Base-T Ports (▼)			
21-24	Green	On	The 1000 Mbps link is up.
	Amber	On	The 100 Mbps link is up.
	Green/Amber	Blinking	The system is transmitting/receiving data.
		Off	The link to an Ethernet network is down.
100/1000 Mbps mini-GBIC Ethernet Ports (▲)			

Table 3-2: LEDs (Continued)

LED	COLOR	STATUS	DESCRIPTION
1-24	Green	On	The 1000 Mbps link is up.
	Amber	On	The 100 Mbps link is up.
	Green/Yellow	Blinking	The system is transmitting/receiving data.
		Off	The link to an Ethernet network is down.
1/10 GbE mini-GBIC Ethernet Uplink Ports (▲)			
25, 26	Green	On	The 1 Gbps link is up.
	Amber	On	The 10 Gbps link is up.
	Green/Amber	Blinking	The system is transmitting/receiving data.
		Off	The link to an Ethernet network is down.

Front Matter

Chapter 4

4.1 Overview

This chapter describes how to show an overview of the traffic flowing on all ports and detailed statistics for each port. Use the:

- **Traffic Overview** screen to see an overview of the traffic flowing on all ports.
- **Detailed Statistics** screen to see individual port statistics.

4.2 Traffic Overview

Use the **Traffic Overview** sub-menu to see the traffic statistics for all switch ports.

To show an overview of traffic statistics, click **Configuration > Port > Traffic Overview**.

Port Statistics Overview									Auto-refresh <input type="checkbox"/>	Refresh	Clear
Port	Packets		Bytes		Errors		Drops		Filtered		
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received		
1	0	0	0	0	0	0	0	0	0		
2	0	0	0	0	0	0	0	0	0		
3	0	0	0	0	0	0	0	0	0		
4	0	0	0	0	0	0	0	0	0		
5	0	0	0	0	0	0	0	0	0		
6	0	0	0	0	0	0	0	0	0		
7	0	0	0	0	0	0	0	0	0		
8	0	0	0	0	0	0	0	0	0		
9	0	0	0	0	0	0	0	0	0		
10	0	0	0	0	0	0	0	0	0		
11	0	0	0	0	0	0	0	0	0		
12	0	0	0	0	0	0	0	0	0		
13	0	0	0	0	0	0	0	0	0		
14	0	0	0	0	0	0	0	0	0		
15	0	0	0	0	0	0	0	0	0		
16	0	0	0	0	0	0	0	0	0		
17	0	0	0	0	0	0	0	0	0		
18	0	0	0	0	0	0	0	0	0		
19	0	0	0	0	0	0	0	0	0		
20	0	0	0	0	0	0	0	0	0		
21	0	0	0	0	0	0	0	0	0		
22	0	0	0	0	0	0	0	0	0		
23	0	0	0	0	0	0	0	0	0		
24	13575	7651	2735574	4889009	0	0	427	0	427		
25	517	0	357168	0	517	0	492	0	492		
26	839	9	679532	1060	839	0	817	0	817		
27	0	0	0	0	0	0	0	0	0		

Figure 4-1. Configuration > Port > Traffic Overview

Table 4-1: Configuration > Port > Traffic Overview

LABEL	DESCRIPTION
Port	This identifies the Ethernet port. Click a port number to display the Detailed Statistics screen. See “Detailed Statistics” on page 7.
Packets	These fields shows the number of received and transmitted packets per port.
Bytes	These fields show the number of received and transmitted bytes per port.
Errors	These fields show the number of frames received in error and the number of incomplete transmissions per port.
Drops	These fields show the number of frames discarded due to ingress or egress congestion.
Filtered	This field shows the number of received frames filtered by the switch forwarding process.

4.3 Status: Port Details

Use the **Detailed Statistics** sub-menu to see per-port traffic statistics.

To show detailed statistics:

1. Click **Configuration > Port > Detailed Statistics**.
2. Select the port number from the **Port Index** drop-down box to show detailed port statistics for that port.

Detailed Port Statistics Port 1			
Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	0	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	0
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

Figure 4-2. Configuration > Port > Detailed Statistics

The following table describes the labels in this screen.

Table 4-2: Configuration > Port > Detailed Statistics

LABEL	DESCRIPTION
Receive Total and Transmit Total	
Rx and Tx Packets	These fields show the number of received and transmitted (good and bad) packets.
Rx and Tx Octets	These fields show the number of received and transmitted (good and bad) byte. This includes the FCS, but excludes framing bits.
Rx and Tx Unicast	These fields show the number of received and transmitted (good and bad) unicast packets.
Rx and Tx Multicast	These fields show the number of received and transmitted (good and bad) multicast packets.
Rx and Tx Broadcast	These fields show the number of received and transmitted (good and bad) broadcast packets.
Rx and Tx Pause	These fields show the number of received and transmitted pause frames.
Receive and Transmit Size Counters	These fields show the number of received and transmitted (good and bad) packets categorized by size.
Receive and Transmit Queue Counters	These fields show the number of received and transmitted packets per input and output queue.
Receive Error Counters	
Rx Drops	This field shows the number of frames dropped due to ingress or egress congestion.
Rx CRC/Alignment	This field shows the number of frames received with CRC or alignment errors.
Rx Undersize	This field shows the number of frames smaller than 64 bytes received with valid CRCs.
Rx Oversize	This field shows the number of frames bigger than the configured maximum frame size received with valid CRCs.

Table 4-2: Configuration > Port > Detailed Statistics

LABEL	DESCRIPTION
Rx Fragments	This field shows the number of frames smaller than 64 bytes received with invalid CRCs.
Rx Jabber	This field shows the number of frames bigger than the configured maximum frame size received with invalid CRCs.
Rx Filtered	This field shows the number of received frames filtered by the forwarding process.
Transmit Error Counters	
Tx Drops	This field shows the number of frames dropped due to output buffer congestion.
Tx Late/Exc. Coll.	This field shows the number of frames dropped due to excessive or late collisions.

Front Matter

Chapter 5

5.1 Overview

This chapter covers basic switch settings in the System Information, General Setup, VLANs, IP Setup and Port Configuration sections.

The System Information section describes general switch information (such as firmware version number). The general setup section describes how to configure general switch identification information. The general setup section also describes how to set the system time manually or get the current time and date from an external server when you turn on your switch. The real time is then displayed in the switch logs. The VLANs section describes how to configure VLANs. The IP Setup section describes how to configure a switch IP address in each routing domain, subnet mask(s) and DNS (domain name server) for management purposes.

Web management screens have some common elements that are described here once.

- **Auto-refresh:**

Check this checkbox to configure the Web interface to refresh the screen regularly.

- **Refresh:**

Click this button to refresh the screen immediately.

- **Clear:**

Click this button to clear the entries in this screen.

- **|<:**

Click this button to go to the first entry.

- **<<:**

Click this button to page back through the entries.

- **>>:**

Click this button to page forward through the entries.

- **>>|:**

Click this button to go to the last entry.

- **Save:**

Click this button to save changes.

- **Reset:**

Click this button to undo any changes made locally and revert to previously saved values.

- **Cancel:**

Click this button to undo any changes made locally and return to the previous page.

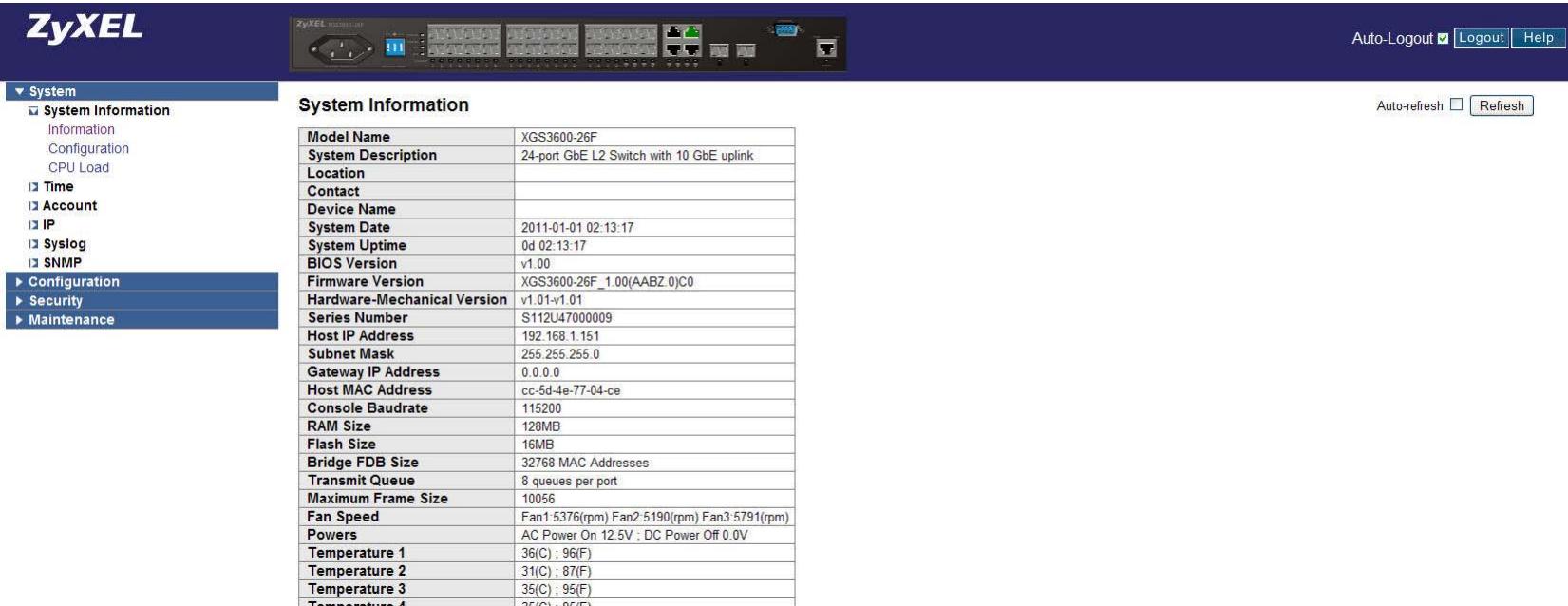
5.1.1 What You Can Do

- Use the **System > System Information > Information** screen to check the firmware version number.
- Use the **System > System Information > Configuration** and **System > Time > Manual** screens to configure the system name and time.
- Use the **Configuration > VLAN > VLAN membership** screen to configure VLANs.
- Use the **System > IP > IPv4** screen to configure the switch IPv4 address, default gateway device, the default domain name server and the management VLAN ID.
- Use the **Configuration > Port > Configuration** screen to configure switch port settings.

5.2 System Information

The System Information screen appears after login. This screen provides a basic overview of the state of the switch, including the software version used, host MAC address, and switch serial number. This information helps support personnel to diagnose a malfunction.

Click **System > System Information > Information** to show the System Information screen.



The screenshot shows the ZyXEL web interface with a dark blue header. The header includes the ZyXEL logo, a navigation bar with icons for Home, System, Network, Security, and Maintenance, and a status bar with 'Auto-Logout' and 'Logout/Help' buttons. The main content area has a left sidebar with a tree view of system categories: System (selected), Configuration (expanded), and Maintenance. The 'Information' sub-item under 'System' is also selected. The main content area is titled 'System Information' and contains a table of system parameters. The table includes the following data:

Model Name	XGS3600-26F
System Description	24-port GbE L2 Switch with 10 GbE uplink
Location	
Contact	
Device Name	
System Date	2011-01-01 02:13:17
System Uptime	0d 02:13:17
BIOS Version	v1.00
Firmware Version	XGS3600-26F_1.00(AABZ.0)C0
Hardware-Mechanical Version	v1.01-v1.01
Series Number	S112U4700009
Host IP Address	192.168.1.151
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
Host MAC Address	cc-5d-4e-77-04-ce
Console Baudrate	115200
RAM Size	128MB
Flash Size	16MB
Bridge FDB Size	32768 MAC Addresses
Transmit Queue	8 queues per port
Maximum Frame Size	10056
Fan Speed	Fan1:5376(rpm) Fan2:5190(rpm) Fan3:5791(rpm)
Powers	AC Power On 12.5V ; DC Power Off 0.0V
Temperature 1	36(C) ; 96(F)
Temperature 2	31(C) ; 87(F)
Temperature 3	35(C) ; 95(F)
Temperature 4	35(C) ; 95(F)

Figure 5-1. System > System Information > Information

The following table describes the labels in this screen.

Table 5-1: System > System Information > Information

LABEL	DESCRIPTION
Model Name	This field shows the model number of the device.
System Description	This field shows a short description of the device.
Location	This field shows the user-defined location of the device.
Contact	This field shows the user-defined contact information of the person responsible for maintaining this device.
Device Name	This field shows the user-defined system name. This is usually the fully-qualified domain name (FQDN).
System Date	This field shows the system time of the device. The format is YYYY-MM-DD HH:MM:SS.
System Uptime	This field shows the accumulated time since the device was powered up.
BIOS Version	This field shows the BIOS version in the device.
Firmware Version	This field shows the firmware version in the device.
Hardware-Mechanical Version	This shows the electronic and mechanical versions of the device. The value before the hyphen is the version of the electronics; the value after the hyphen is the version of mechanical hardware.
Serial Number	This shows the serial number of the device.
Host IP Address	This shows the IP address of the device.
Subnet Mask	This shows the subnet mask of the device.
Gateway IP Address	This shows the IP address that the device uses for its gateway.

Table 5-1: System > System Information > Information

LABEL	DESCRIPTION
Host MAC Address	This shows the MAC address of the management agent in this device.
Console Baud rate	This shows the baud rate of the device's console port.
RAM Size	This shows the amount of RAM in this device.
Flash Size	This shows the amount of flash memory in this device.
Bridge FDB Size	This shows the total number of entries that the device can hold in its forwarding database.
Transmit Queue	This shows the number of hardware priority transmit queues per port on this device.
Maximum Frame Size	This shows the maximum frame size of the device.
Fan Speed	This shows the speeds of fan 1, 2 and 3.
Powers	This shows the voltage supplied by the internal AC power supply and the external DC power input.
Temperature 1 to 4	This shows the temperature of four important chips in the device.

5.3 General Setup

Use the **System Information** screen to configure system identification fields. To configure system information:

1. Click **System > System Information > Configuration**.
2. Enter System Contact, System Name, System Location information.
3. Click **Save** to save the configuration or **Reset** to discard your changes.

System Information Configuration

System Contact	
System Name	
System Location	

Figure 5-2. System > System Information > Configuration

Use the **Time** sub-menu to set the time manually or configure NTP.

To manually configure the time:

1. Click **System > Time > Manual**. The Time Configuration screen appears.
2. Enter the time parameters.
3. Click **Save**.

Time Configuration

Clock Source: <input checked="" type="radio"/> Use Local Settings <input type="radio"/> Use NTP Server	
Local Time: 2011-01-01 01:45:10 YYYY-MM-DD HH:MM:SS	
Time Zone Offset: 0 min	
Daylight Savings: <input type="checkbox"/> Enable	
Time Set Offset: 60 min. (Range: 1 - 1440, Default: 60)	
Daylight Savings Type: <input checked="" type="radio"/> By dates <input type="radio"/> Recurring	
From: YYYY-MM-DD HH:MM	
To: YYYY-MM-DD HH:MM	
From: Day: Sun Week: First Month: Jan Time: 00:00 HH:MM	
To: Day: Sun Week: First Month: Jan Time: 00:00 HH:MM	
<input type="button" value="Save"/> <input type="button" value="Reset"/>	
Time & Date 2011-01-01 01:45:10	

Figure 5-3. System > Time > Manual

The following table describes the labels in these screens.

Table 5-2: System Information and Time Configuration

LABEL	DESCRIPTION
System Contact	This field identifies the person responsible for this device and their contact information. The maximum length of text is 255 characters and each character can have an ASCII code of 32 to 126.
System Name	This field contains the user-defined system name. This is usually the fully-qualified domain name (FQDN). This must begin with a letter, end with a letter or digit and have letters, digits or hyphens in between. The maximum length of text is 255 characters.

Table 5-2: System Information and Time Configuration

LABEL	DESCRIPTION
System Location	This shows the location of the device (e.g. telephone closet, 3rd floor). The maximum length of text is 255 characters and each character can have an ASCII code of 32 to 126.
Clock Source	Select Use Local Settings or Use NTP Server to set the time from the device's onboard clock or from a remote NTP server.
Local Time	Use this field to set the device's onboard clock.
Time Zone Offset	Use this field to configure the time zone offset relative to UTC/GMT. This is also used when NTP synchronizes time.
Daylight Savings	Use this check box to enable or disable daylight saving mode. In daylight saving mode, the time will be offset by the Time Set Offset value between the From and To times.
Time Set Offset	Use this field to configure the daylight saving time offset. If this is non-zero, the From and To fields must be configured to enable daylight saving mode.
Daylight Savings Type	Select By dates or Recurring to configure how the From and To fields are used to define daylight saving time. Select By dates to start and finish daylight saving on fixed dates. Select Recurring to start and finish daylight saving on a day of the month.
From	Use this field to configure the start of daylight saving time. The top From field is active if the By dates radio button is selected in Daylight Savings Type otherwise the bottom From field is active.
To	Use this field to configure the end of daylight saving time. The top To field is active if the By dates radio button is selected in Daylight Savings Type otherwise the bottom To field is active.

5.4 VLANs

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLANs, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In MTU (Multi-Tenant Unit) applications, VLANs are vital in providing isolation and security among the subscribers. When properly configured, VLANs prevent one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLANs also increase network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Note:

VLANs are unidirectional; they only govern outgoing traffic.

Use the **VLAN** sub-menu to configure which ports can communicate with other ports. Use the **VLAN Membership** sub-menu to add, delete or modify VLANs.

To configure VLAN membership:

1. Click **Configuration > VLAN > VLAN membership**.
2. Click **Add New VLAN**.
3. Configure the parameters.
4. Click **Save**.

VLAN Membership Configuration

Start from VLAN with entries per page.

Delete	VLAN ID	VLAN Name	Port Members																										
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
<input type="checkbox"/>	1	default	<input checked="" type="checkbox"/>																										

[Add New VLAN](#) [Save](#) [Reset](#)

Figure 5-4. Configuration > VLAN > VLAN membership

The following table describes the labels in this screen.

Table 5-3: Configuration > VLAN > VLAN membership

LABEL	DESCRIPTION
VLAN ID	Use this field to configure the identity of this VLAN.
VLAN Name	Use this field to configure the name of VLAN. The VLAN name can only contain alphabetic or numeric characters and should contain at least one alphabetic character.
Port Members	Use these check boxes to configure membership for each VLAN ID. No ports are members by default.

5.5 IP Setup

Use the IP Setup screen to configure the switch IP address, default gateway device, the default domain name server and the management VLAN ID. The default gateway specifies the IP address of the default gateway (next hop) for outgoing traffic.

5.5.1 Management IP Addresses

The switch needs an IP address for it to be managed over the network. The factory default static IP address is 192.168.1.1. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0. Inband configuration applies to non-management ports and outband configuration applies only to the management port.

The switch gets its management IPv4 configuration via DHCP by default. If there is no DHCP server, the switch uses the static IP configuration.

To set the IPv4 configuration:

1. Click **System > IP > IPv4**.
2. Specify the IPv4 settings, and enable the **DNS Proxy** service if required.
3. Click **Save**.

IP Configuration

	Configured	Current
DHCP Client	<input type="checkbox"/>	<input type="button" value="Renew"/>
Inband IP Address	192.168.1.151	192.168.1.151
Inband IP Mask	255.255.255.0	255.255.255.0
Inband IP Gateway	0.0.0.0	0.0.0.0
Inband VLAN ID	1	1
Inband Default Gateway	<input type="checkbox"/>	
Outband IP Address	192.168.0.1	192.168.0.1
Outband IP Mask	255.255.255.0	255.255.255.0
Outband IP Gateway	192.168.0.254	192.168.0.254
DNS Server	0.0.0.0	0.0.0.0

IP DNS Proxy Configuration

DNS Proxy	<input type="checkbox"/>
-----------	--------------------------

Figure 5-5. System > IP > IPv4

The following table describes the labels in this screen.

Table 5-4: System > IP > IPv4

LABEL	DESCRIPTION
DHCP Client	Use this check box to enable or disable the DHCP client. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the static IP settings will be used. The DHCP client will announce the configured System Name as host name to provide DNS lookup.
IP Address	Use this field to set the management IPv4 address of this switch.
IP Mask	Use this field to set the IPv4 mask of this switch.
IP Gateway	Use this field to set the IPv4 address of the default gateway.

Table 5-4: System > IP > IPv4

LABEL	DESCRIPTION
VLAN ID	Use this field to set the management VLAN ID. The allowed range is 1 to 4095.
DNS Server	Use this field to set the IPv4 address of the DNS Server.
DNS Proxy	Use this check box to enable or disable the DNS Proxy. When DNS Proxy is enabled the device appears as a DNS resolver to DNS clients connected to the device. Only valid DNS requests are relayed to the DNS server on behalf of DNS clients connected to the device. This helps to protect DNS clients against attack.

5.6 Port Configuration

Use the **Configuration** sub-menu to configure the speed, flow control and power-saving characteristics of each port.

To configure a port:

1. Click **Configuration > Port > Configuration**.
2. Specify the port parameters.

3. Click **Save**.

Port Configuration

Refresh

Port	Link	Current	Speed	Flow Control			Maximum	Excessive	Power
			Configured	Current Rx	Current Tx	Configured			
*			<>				10056	<>	<>
1	Down	Auto					10056		
2	Down	Auto					10056		
3	Down	Auto					10056		
4	Down	Auto					10056		
5	Down	Auto					10056		
6	Down	Auto					10056		
7	Down	Auto					10056		
8	Down	Auto					10056		
9	Down	Auto					10056		
10	Down	Auto					10056		
11	Down	Auto					10056		
12	Down	Auto					10056		
13	Down	Auto					10056		
14	Down	Auto					10056		
15	Down	Auto					10056		
16	Down	Auto					10056		
17	Down	Auto					10056		
18	Down	Auto					10056		
19	Down	Auto					10056		
20	Down	Auto					10056		
21	Down	SFP_Auto_AMS		✗	✗		10056	Discard	Disabled
22	Down	SFP_Auto_AMS		✗	✗		10056	Discard	Disabled
22	Down	SFP_Auto_AMS		✗	✗		10056	Discard	Disabled
23	Down	SFP_Auto_AMS		✗	✗		10056	Discard	Disabled
24	1Gfdx	SFP_Auto_AMS		✗	✗		10056	Discard	Disabled
25	Down	10Gbps FDX					10056		
26	Down	10Gbps FDX					10056		
27	Down	Auto					10056	Discard	Disabled

Save Reset

Figure 5-6. Configuration > Port > Configuration

The following table describes the labels in this screen.

Table 5-5: Configuration > Port > Configuration

LABEL	DESCRIPTION
Port	This field shows the port number for this row.
Link	This field shows the current link state. Green indicates the link is up and red that it is down.
Current Link Speed	This field shows the current link speed.
Configured Link Speed	Use this drop-down box to select a fixed link speed.
Flow Control	Check the Configured column to use pause frames for flow control. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. If the configured link speed is auto, the current Rx and Tx fields show the flow control capabilities of the link partner. If the configured link speed is fixed, the current Rx and Tx fields reflect that setting. The current Rx and Tx settings are determined by the result of the last Auto-Negotiation. Flow control is not possible for half duplex (HDX) link speeds.
Maximum Frame Size	Use this field to configure the maximum frame size, including Frame Check Sequence (FCS) allowed for the port.
Excessive Collision Mode	<p>Use this drop-down box to configure port transmit collision behavior. Possible collision modes are:</p> <ul style="list-style-type: none"> ■ Discard: Discard frame after 16 collisions (default). ■ Restart: Restart backoff algorithm after 16 collisions.

Table 5-5: Configuration > Port > Configuration

LABEL	DESCRIPTION
Power Control	<p>Use this drop-down box to configure power-saving options. Possible power control modes are:</p> <ul style="list-style-type: none">■ Disabled: All power saving mechanisms disabled.■ ActiPHY: Link down power saving enabled.■ PerfectReach: Link up power saving enabled.■ Enabled: Both link up and link down power savings enabled.

Part II: Front Matter

Overview

This user's manual explains how to install, configure and manage the MGS3600-24F/XGS3600-26F/XGS3600-28F using the web interface via Ethernet ports.

MGS3600-24F/XGS3600-26F/XGS3600-28F switches are affordable, next generation, L2+ managed switches that provide a reliable infrastructure for your business network. These switches have intelligent features that improve the availability of critical business applications, protect sensitive information, and optimize network bandwidth. They provide the ideal combination of features and affordability for the entry level networking requirements of small business or enterprise applications to help create a more efficient and better-connected workforce.

MGS3600-24F/XGS3600-26F/XGS3600-28F switches provide the following features.

- Twenty 100/1000 SFP ports
- Four dual personality ports (10/100/1000 BASE-T and 100/1000M SFP)
- L2+ capability for better manageability, security, QoS, and performance
- Guest, voice, port-based, tag-based and protocol-based VLANs
- 802.3az Energy Efficient Ethernet
- A 32K MAC table
- IPv6/IPv4 dual stack
- sFlow
- Easy port configuration for easy connection of IP Phones, IP Cameras or wireless environments

Initial Configuration

The MGS3600-24F/XGS3600-26F/XGS3600-28F allows only one administrator to configure the system at any given time. If more than one user logs in as admin, only the first user to log in is allowed to configure the system; other users can only monitor the system. Non-admin users can only ever monitor the system. A maximum of three users can log in simultaneously.

The default management interface configuration of the MGS3600-24F/XGS3600-26F/XGS3600-28F is as follows.

Table 6-1: Default Management Interface Configuration

DHCP Client	Enabled
Static IP Address	192.168.1.1
Static Subnet Mask	255.255.255.0
Static Default Gateway	192.168.1.254
Username	admin
Password	<Blank password>

Note:

The default admin password is blank, so simply press enter at the password prompt.

The MGS3600-24F/XGS3600-26F/XGS3600-28F Web interface can be accessed over IPv4 or IPv6.

This switch supports a neutral web browser interface. We recommend a minimum of Microsoft IE 6.0, Netscape 7.1 or Firefox 1.00 and a screen resolution of 1024x768 for optimal results.

The MGS3600-24F/XGS3600-26F/XGS3600-28F gets its IP configuration via DHCP by default. If there is no DHCP server, the switch uses the static IP configuration.

Front Matter

Chapter 6

6.1 System Configuration

This chapter describes the System Information, Time, Account, IP, Syslog and SNMP sub-menus.

6.2 System Information

The System Information screen appears after login. This screen provides a basic overview of the state of the switch, including the software version used, host MAC address, and switch serial number. This information helps support personnel to diagnose a malfunction.

6.2.1 Information

Click **System > System Information > Information** to show the System Information screen.

Parameter description

- **Model Name:**

This field shows the model number of the device.

- **System Description:**

This field shows a short description of the device.

- **Location:**

This field shows the user-defined location of the device.

- **Contact:**

This field shows the user-defined contact information of the person responsible for maintaining this device.

- **Device Name:**

This field shows the user-defined system name. This is usually the fully-qualified domain name (FQDN).

- **System Date:**

This field shows the system time of the device. The format is YYYY-MM-DD HH:MM:SS.

- **System Uptime:**

This field shows the accumulated time since the device was powered up.

- **BIOS Version:**

This field shows the BIOS version in the device.

- **Firmware Version:**

This field shows the firmware version in the device.

- **Hardware-Mechanical Version:**

This shows the electronic and mechanical versions of the device. The value before the hyphen is the version of the electronics; the value after the hyphen is the version of mechanical hardware.

- **Serial Number:**

This shows the serial number of the device.

- **Host IP Address:**

This shows the IP address of the device.

- **Subnet Mask:**

This shows the subnet mask of the device.

- **Gateway IP Address:**

This shows the IP address that the device uses for its gateway.

- **Host MAC Address:**

This shows the MAC address of the management agent in this device.

- **Console Baudrate:**

This shows the baud rate of the device's console port.

- **RAM Size:**

This shows the amount of RAM in this device.

- **Flash Size:**

This shows the amount of flash memory in this device.

- **Bridge FDB Size:**

This shows the total number of entries that the device can hold in its forwarding database.

- **Transmit Queue:**

This shows the number of hardware priority transmit queues per port on this device.

- **Maximum Frame Size:**

This shows the maximum frame size of the device.

- **Fan Speed:**

This shows the speeds of fan 1, 2 and 3.

- **Powers:**

This shows the voltage supplied by the internal AC power supply and the external DC power input.

- **Temperature 1 to 4:**

This shows the temperature of four important chips in the device.

6.2.2 Configuration

Use this screen to configure system identification fields. To configure system information:

1. Click **System > System Information > Configuration**.
2. Enter System Contact, System Name, System Location information.
3. Click **Save** to save the configuration or **Reset** to discard your changes.

Parameter description

- **System Contact:**

This field identifies the person responsible for this device and their contact information. The maximum length of text is 255 characters and each character can have an ASCII code of 32 to 126.

- **System Name:**

This field contains the user-defined system name. This is usually the fully-qualified domain name (FQDN). This must begin with a letter, end with a letter or digit and have letters, digits or hyphens in between. The maximum length of text is 255 characters.

- **System Location:**

This shows the location of the device (e.g. telephone closet, 3rd floor). The maximum length of text is 255 characters and each character can have an ASCII code of 32 to 126.

6.2.3 CPU Load

Use this screen to see a graph (rendered by SVG) of how the CPU is being used. The load is shown as a points that are the average load over 100 ms, 1 second and 10 second intervals.

To see the CPU Load, Click **System > System Information > CPU Load**.

6.3 Time

Use the **Time** sub-menu to set the time manually or configure NTP.

6.3.1 Manual

To manually configure the time:

1. Click **System > Time > Manual**. The Time Configuration screen appears.
2. Enter the time parameters.
3. Click **Save**.

Parameter description

- **Clock Source:**
Select **Use Local Settings** or **Use NTP Server** to set the time from the device's onboard clock or from a remote NTP server.
- **Local Time:**
Use this field to set the device's onboard clock.
- **Time Zone Offset:**
Use this field to configure the time zone offset relative to UTC/GMT. This is also used when NTP synchronizes time.
- **Daylight Savings:**
Use this check box to enable or disable daylight saving mode. In daylight saving mode, the time will be offset by the **Time Set Offset** value between the **From** and **To** times.
- **Time Set Offset:**
Use this field to configure the daylight saving time offset. If this is non-zero, the **From** and **To** fields must be configured to enable daylight saving mode.
- **Daylight Savings Type:**

Select **By dates** or **Recurring** to configure how the **From** and **To** fields are used to define daylight saving time. Select **By dates** to start and finish daylight saving on fixed dates. Select **Recurring** to start and finish daylight saving on a day of the month.

- **From:**

Use this field to configure the start of daylight saving time. The top **From** field is active if the **By dates** radio button is selected in **Daylight Savings Type** otherwise the bottom **From** field is active.

- **To:**

Use this field to configure the end of daylight saving time. The top **To** field is active if the **By dates** radio button is selected in **Daylight Savings Type** otherwise the bottom **To** field is active.

6.3.2 NTP

Network Time Protocol (NTP) synchronizes local clocks across a network based on UTC/GMT. To configure the device to use NTP:

1. Click **System > Time > Manual**. The **Time Configuration** screen appears.
2. Select **Use NTP Server**, enter the **Time Zone Offset** and then click **Save**.
3. Click the **NTP** submenu. The **NTP Configuration** screen appears.
4. Enter an NTP server IP address in **Server1**. Repeat this step for up to 4 more NTP server IP addresses.
5. Click **Save**.

Note:

If you use NTP mode and select the built-in NTP time server or manually specify a user-defined NTP server along with a time zone, the switch will sync the time shortly after pressing the **Apply** button. Though it synchronizes the time automatically, NTP does not update the time periodically without user intervention.

Note:

You must enter the **Time Zone Offset** in **System > Time > Manual** before performing a time sync via NTP because the switch will calculate local time from the time zone offset and the NTP time. The time zone range is from -12 to +13 in steps of 1 hour. The default time zone offset is +8 hours relative to UTC/GMT.

Parameter description

- **Server 1 to 5:**

Use these fields to enter the IPv4 or IPv6 IP addresses of the NTP servers.

An IPv6 address is a 128-bit value represented by eight colon-separated hexadecimal strings of four digits. An example address is 'fe80::215:c5ff:fe03:4dc7'. The double colon symbol '::' is a shorthand way of representing multiple strings of contiguous zeros, but it can only appear once. The double colon symbol can also be used to represent an IPv4 address. For example, '::192.1.2.34'.

6.4 Account

Use the **Account** sub-menu to configure Web Configurator and CLI users and the privilege levels of each group that runs on the switch.

6.4.1 Users

This page provides an overview of the current users.

Only the administrator can create, modify or delete usernames and passwords. The administrator can modify the passwords of guests without confirming the password but confirmation is necessary to modify administrator-equivalent identities. Guests can only modify their passwords. Guests must confirm their identity in the Authorization field before configuring the username and password. There is only one administrator, and this administrator cannot be deleted. Up to 4 guest accounts can be created.

To add a user account:

1. Click **System > Account > User**. The **Users Configuration** screen appears.
2. Click **Add new user**. The **Add User** screen appears.
3. Enter the new user name, password and privilege level.
4. Click **Save**.

Parameter description

- **User Name:**

Use this field to enter the identity of the user. This is also a link to the Edit User screen.

- **Password:**

Use this field to enter the password. Passwords can be up to 255 characters, each of which with ASCII codes between 32 to 126.

- **Password (again):**

Use this field to confirm the password.

- **Privilege Level:**

Use this field to enter the privilege level of the user. The allowed range is 1 to 15. A privilege level of 15 (all groups) has full control of the device. The access granted to other privilege levels depends on the group. The user's privilege level must be the same or greater than the group privilege level to have the access of that group. By default, for most groups, privilege level 5 has read-only access and privilege level 10 has read-write access. System maintenance (software upload, factory defaults, etc.) needs user privilege level 15. Privilege level 15 is used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

6.4.2 Privilege Level

This screen provides an overview of the privilege levels of each group.

To configure group privilege levels:

1. Click **System > Account > Privilege Level**. The **Privilege Level** screen appears.
2. Use the drop-down boxes under the **Privilege Levels** column to configure the privilege level of each group.
3. Click **Save**.

Parameter description

- **Group Name:**

This column lists privilege level groups. Most privilege level groups consist of a single module (e.g. LACP, RSTP or QoS), but the following groups contain more than one module.

- **System:** Contact, Name, Location, Timezone, Log.
- **Security:** Authentication, System Access Management, Port (802.1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection and IP source guard.
- **IP:** Everything except ping.
- **Port:** Everything except VeriPHY.
- **Diagnostics:** Ping and VeriPHY.
- **Maintenance:**
 - CLI:- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load.
 - Web:- Users, Privilege Levels and everything in Maintenance.
- **Debug:** Only present in the CLI.

- **Privilege Levels:**

Use these fields to configure the authorization privilege level of each group. Every group has an authorization privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (e.g. for clearing of statistics). The user's privilege must be the same or greater than the authorization privilege level to have access to that group.

6.5 IP

Use the **IP** sub-menu to configure DNS Proxy and the host IP address for the management interface. Inband configuration applies to non-management ports and outband configuration applies only to the management port.

6.5.1 IPv4

The switch gets its management IPv4 configuration via DHCP by default. If there is no DHCP server, the switch uses the static IP configuration.

To set the IPv4 configuration:

1. Click **System > IP > IPv4**.
2. Specify the IPv4 settings, and enable the **DNS Proxy** service if required.
3. Click **Save**.

Parameter description

The **Configured** column is used to view or change the IP configuration. The **Current** column is used to show the active IP configuration.

- **DHCP Client:**

Use this check box to enable or disable the DHCP client. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the static IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

- **Inband IP Address or Outband IP Address:**

Use this field to set the management IPv4 address of this switch.

- **Inband IP Mask or Outband IP Mask:**

Use this field to set the IPv4 mask of this switch.

- **Inband IP Gateway or Outband IP Gateway:**

Use this field to set the IPv4 address of the default gateway.

- **Inband VLAN ID:**

Use this field to set the management VLAN ID. The allowed range is 1 to 4095.

- **Inband Default Gateway:**

Check this checkbox to enable the inband default gateway.

- **DNS Server:**

Use this field to set the IPv4 address of the DNS Server.

- **DNS Proxy:**

Use this check box to enable or disable the DNS Proxy. When DNS Proxy is enabled the device appears as a DNS resolver to DNS clients connected to the device. Only valid DNS requests are relayed to the DNS server on behalf of DNS clients connected to the device. This helps to protect DNS clients against attack.

6.5.2 IPv6

Use the **IPv6** sub-menu to configure the host IPv6 address for the management interface.

To set the IPv6 configuration:

1. Click **System > IP > IPv6**.
2. Specify the IPv6 settings.
3. Click **Save**.

Parameter description

The **Configured** column is used to view or change the IPv6 configuration. The **Current** column is used to show the active IPv6 configuration.

- **Auto Configuration:**

Use this check box to enable or disable IPv6 auto-configuration. If auto-configuration fails, the configured IPv6 address is zero. The router may delay responding to a router solicitation for a few seconds, so the total time needed to complete auto-configuration can be significantly longer.

- **Address:**

Use this field to set the IPv6 address of this switch.

An IPv6 address is a 128-bit value represented by eight colon-separated hexadecimal strings of four digits. An example address is 'fe80::215:c5ff:fe03:4dc7'. The double colon symbol '::' is a shorthand way of representing multiple strings of contiguous zeros, but it can only appear once.

- **Prefix:**

Use this field to set the IPv6 prefix of this switch. The allowed range is 1 to 128.

- **Gateway:**

Use this field to set the IPv6 gateway address of this switch.

6.6 SYSLOG

Use the **Syslog** sub-menu to view the system log and configure how system events are logged.

Syslog is a standard for logging program messages. Syslog allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. Syslog is supported by a wide variety of devices and receivers across multiple platforms.

6.6.1 Configuration

This section describes how to configure the Syslog.

To configure Syslog

1. Click **System > Syslog > Configuration**.
2. Specify the syslog parameters.
3. Click **Save**.

Parameter description

- **Server Mode:**

Use this drop-down box to enable or disable sending syslog messages via UDP port 514 to a syslog server. UDP is connectionless, so syslog messages are sent even if the syslog server does not exist.

- **Server Address 1 and 2:**

Use these fields to configure up to two IPv4 syslog server addresses for redundancy. These addresses can be a host name if a DNS server is configured.

- **Syslog Level:**

Use this drop-down box to configure the severity level of the messages that are sent to the syslog server. Possible levels are: Emergency, Alert, Critical, Error, Warning, Notice, Informational and Debug.

6.6.2 Log

Use this sub-menu to view the system log.

To display the system log:

1. Click **System > Syslog > Log**.
2. Enter the level of logging to show, the log entry to show first, and the number of entries per page or click **<<** or **>>** to move to the previous or next entry.

Parameter description

- **ID:**

This shows the ID of the system log entry. Click an ID to see a detailed view of that entry.

- **Level:**

This shows the level of the system log entry. Possible levels are Emergency, Alert, Critical, Error, Warning, Notice, Informational and Debug.

- **Time:**

This shows the time that the log entry was made.

- **Message:**

This shows a summary of the log entry.

6.6.3 Detailed Log

Use this sub-menu to show a detailed view of a log entry.

To display a detailed log entry:

1. Click **System > Syslog > Detailed Log**.
2. Select an ID to see a detailed view of that entry.

Parameter description

- **ID:**

Use this drop-down box to select the ID of the system log entry.

- **Message:**

This shows the details of a log entry.

6.7 SNMP

Use the **SNMP** sub-menu to configure the Simple Network Management Protocol on the device.

SNMP governs communication between SNMP managers and agents. Any SNMP manager can manage devices that have an SNMP agent and a correctly installed Management Information Base (MIB). Most communication is initiated by the SNMP Manager; traps are the only communication initiated by agents.

6.7.1 System

To enable or disable SNMP:

1. Click **System > SNMP > System**.
2. Specify the SNMP parameters.
3. Click **Apply**.

Parameter description

- **SNMP State:**

Use these radio buttons to enable (default) or disable the SNMP agent.

- **Engine ID:**

Use this field to configure the SNMPv3 Engine ID. The Engine ID is a hexadecimal number between 5 and 32 octets long. The fifth octet must not be 00. All users are cleared if the Engine ID is changed.

6.7.2 Communities

Use the **Communities** sub-menu to configure the SNMPv3 community table. Each community must be different from the other communities, and each user name must be different from the other usernames. The maximum number of communities is 4 and the entry index is community.

To configure SNMP Communities:

1. Click **System > SNMP > Communities**.
2. Click **Add new community**.
3. Specify the SNMP community and user name parameters.
4. Click **Save**.

Parameter description

- **Delete:**

Use this check box to mark an entry for deletion. The entry is deleted during the next save.

- **Community:**

Use this field to configure an SNMPv3 community access string. Community strings can be up to 32 characters, each of which with ASCII codes from 33 to 126. The community string is treated as a security name and mapped to an SNMPv1 or SNMPv2c community string.

- **User Name:**

Use this field to configure an SNMPv3 user name. User names can be up to 32 characters, each of which with ASCII codes from 33 to 126.

- **Source IP:**

Use this field to limit access to the SNMP agent in this switch by IP source address.

- **Source Mask:**

Use this field to limit access to the SNMP agent in this switch by IP source subnet.

6.7.3 Users

Use the **Users** sub-menu to configure the SNMPv3 user table. The maximum number of users is ten and the entry index is user name.

To configure SNMP Users:

1. Click **System > SNMP > Users**.
2. Click **Add new user**.
3. Enter the user information.
4. Click **Save**.

Parameter description

- **User Name:**

Use this field to configure a user name. User names can be up to 32 characters, each of which with ASCII codes from 33 to 126.

- **Security Level:**

Use this drop-down box to configure the security level of a new entry. Possible security levels are:

- **NoAuth, NoPriv:** No authentication and no privacy.
- **Auth, NoPriv:** Authentication and no privacy.
- **Auth, Priv:** Authentication and privacy.

The security level of an existing entry can't be changed.

- **Authentication Protocol:**

Use this drop-down box to configure the authentication protocol of a new entry. Possible authentication protocols are:

- **None:** No authentication protocol.
- **MD5:** An optional flag to indicate that this user uses the MD5 authentication protocol.
- **SHA:** An optional flag to indicate that this user uses the SHA authentication protocol.

The authentication protocol of an existing entry can't be changed.

- **Authentication Password:**

Use this field to configure an authentication password phrase. MD5 passwords are 8 to 32 characters long. SHA passwords are 8 to 40 characters long. Each character can be an ASCII code from 33 to 126.

- **Privacy Protocol:**

Use this drop-down box to configure the privacy protocol of a new entry. Possible privacy protocols are:

- **None:** No privacy protocol.
- **DES:** An optional flag to indicate that this user uses the DES authentication protocol.

- **Privacy Password:**

Use this field to configure an privacy password phrase. Passwords are 8 to 32 characters long. Each character can be an ASCII code from 33 to 126.

6.7.4 Groups

Use the **Groups** sub-menu to configure the SNMP group table. The maximum number of groups is two for SNMP v1/v2 or ten for SNMP v3 and the entry index is security model and security name.

To configure SNMP Groups:

1. Click **System > SNMP > Groups**.
2. Click **Add new group**.
3. Enter the group information.
4. Click **Save**.

Parameter description

- **Delete:**

Use this check box to mark an entry for deletion. The entry is deleted during the next save.

- **Security Model:**

Use this drop-down box to configure the security model of a new entry. Possible security models are:

- **v1:** SNMPv1.
- **v2c:** SNMPv2c.
- **usm:** SNMPv3 User-based Security Model (USM).

- **Security Name:**

Use this field to configure a security name. Security names can be up to 32 characters, each of which with ASCII codes from 33 to 126.

- **Group Name:**

Use this field to configure a group name. Group names can be up to 32 characters, each of which with ASCII codes from 33 to 126.

6.7.5 Views

Use the **Views** sub-menu to configure the SNMPv3 view table. The maximum number of views is 28 and the entry indices are view name and OID subtree.

To configure a new view:

1. Click **System > SNMP > Views**.
2. Click **Add new View**.
3. Specify the SNMP View parameters.
4. Click **Save**.

Parameter description

- **Delete:**

Use this check box to mark an entry for deletion. The entry is deleted during the next save.

- **View Name:**

Use this field to configure a view name. View names can be up to 32 characters, each of which with ASCII codes from 33 to 126.

- **View Type:**

Use this drop-down box to configure the view type of a new entry. Possible view types are:

- **included:** This view is included.
- **excluded:** This view is excluded.

In general for every excluded view, there should be another included view to cover the OID subtree of the excluded view entry.

- **OID Subtree:**

Use this field to configure the root of the view. The allowed OID length is 1 to 128 characters. Each node can be a whole decimal number or an asterisk(*) .

6.7.6 Access

Use the **Access** sub-menu to configure SNMPv3 access table. The maximum number of groups is 14 and the entry indices are group name, security model and security level.

To add a new SNMP Access entry:

1. Click **System > SNMP > Access**.
2. Click **Add new Access**.
3. Specify the SNMP Access parameters.
4. Click **Save**.

Parameter description

- **Delete:**

Use this check box to mark an entry for deletion. The entry is deleted during the next save.

- **Group Name:**

Use this field to configure a group name. Group names can be up to 32 characters, each of which with ASCII codes from 33 to 126.

- **Security Model:**

Use this drop-down box to configure the security model of a new entry. Possible security models are:

- **any:** Any security model accepted.
- **v1:** SNMPv1.
- **v2c:** SNMPv2c.
- **usm:** SNMPv3 User-based Security Model (USM).

- **Security Level:**

Use this drop-down box to configure the security level of a new entry. Possible security levels are:

- **NoAuth, NoPriv:** No authentication and no privacy.
- **Auth, NoPriv:** Authentication and no privacy.
- **Auth, Priv:** Authentication and privacy.

- **Read View Name:**

Use this drop-down box to configure the SNMP view used to read MIB values.

- **Write View Name:**

Use this drop-down box to configure the SNMP view used to read and write MIB values.

6.7.7 Trap

Use the **Trap** sub-menu to configure the SNMP trap table. The maximum number of traps is 6.

To configure an SNMP Trap:

1. Click **System > SNMP > Trap** to display the SNMP Trap Hosts Configuration table.
2. Click an entry number to display or modify it.
3. Specify the Trap parameters.
4. Click **Save**.

Parameters description:

- **Delete:**

Use this check box to mark an entry for deletion. The entry is deleted during the next save.

- **Trap Version:**

Use this drop-down box to configure an SNMP v2c or v3 trap.

- **Server IP:**

Use this field to configure the IP address of the host that will receive the trap.

- **UDP Port:**

Use this field to configure the UDP port number that traps are sent to. The default is port is 162.

- **Community / Security Name:**

Use this field to configure an SNMPv3 community access string. Community strings can be up to 32 characters, each of which with ASCII codes from 33 to 126. The community string is treated as a security name and mapped to an SNMPv1 or SNMPv2c community string.

- **Severity Level:**

Use this drop-down box to configure the severity level of the messages that are sent as traps. Possible levels are: Emergency, Alert, Critical, Error, Warning, Notice, Informational and Debug.

- **Security Level:**

Use this drop-down box to configure the security level of a new entry. Possible security levels are:

- **NoAuth, NoPriv:** No authentication and no privacy.

- **Auth, NoPriv:** Authentication and no privacy.
- **Auth, Priv:** Authentication and privacy.
- **Authentication Protocol:**
Use this drop-down box to configure the authentication protocol of a new entry. Possible authentication protocols are:
 - **None:** No authentication protocol.
 - **MD5:** An optional flag to indicate that this user uses the MD5 authentication protocol.
 - **SHA:** An optional flag to indicate that this user uses the SHA authentication protocol.
- **Authentication Password:**
Use this field to configure an authentication password phrase. MD5 passwords are 8 to 32 characters long. SHA passwords are 8 to 40 characters long. Each character can be an ASCII code from 33 to 126.
- **Privacy Protocol:**
Use this drop-down box to configure the privacy protocol of a new entry. Possible privacy protocols are:
 - **None:** No privacy protocol.
 - **DES:** An optional flag to indicate that this user uses the DES authentication protocol.
- **Privacy Password:**
Use this field to configure an privacy password phrase. Passwords are 8 to 32 characters long. Each character can be an ASCII code from 33 to 126.

Front Matter

Chapter 7

7.1 Configuration

This chapter describes the sub-menus used to configure the core functions of this device.

7.2 Port

Use the **Port** sub-menu to configure the physical and data-link layer characteristics of each port.

7.2.1 Configuration

Use the **Configuration** sub-menu to configure the speed, flow control and power-saving characteristics of each port.

To configure a port:

1. Click **Configuration > Port > Configuration**.
2. Specify the port parameters.
3. Click **Save**.

Parameter description

- **Port:**

This field shows the port number for this row.

- **Link:**

This field shows the current link state. Green indicates the link is up and red that it is down.

- **Current Link Speed:**

This field shows the current link speed.

- **Configured Link Speed:**

Use this drop-down box to select a fixed link speed or:

- **Auto** to select the highest speed that is compatible with a link partner.
- **Disabled** to disable the switch port operation.

- **Flow Control:**

Check the **Configured** column to use pause frames for flow control. The **Current Rx** column indicates whether pause frames on the port are obeyed, and the **Current Tx** column indicates whether pause frames on the port are transmitted. If the configured link speed is auto, the

current Rx and Tx fields show the flow control capabilities of the link partner. If the configured link speed is fixed, the current Rx and Tx fields reflect that setting. The current Rx and Tx settings are determined by the result of the last Auto-Negotiation. Flow control is not possible for half duplex (HDX) link speeds.

- **Maximum Frame Size:**

Use this field to configure the maximum frame size, including Frame Check Sequence (FCS) allowed for the port.

- **Excessive Collision Mode:**

Use this drop-down box to configure port transmit collision behavior. Possible collision modes are:

- **Discard:** Discard frame after 16 collisions (default).
- **Restart:** Restart backoff algorithm after 16 collisions.

- **Power Control:**

Use this drop-down box to configure power-saving options. Possible power control modes are:

- **Disabled:** All power saving mechanisms disabled.
- **ActiPHY:** Link down power saving enabled.
- **PerfectReach:** Link up power saving enabled.
- **Enabled:** Both link up and link down power savings enabled.

7.2.2 Port Description

Use the **Port Description** sub-menu to label ports. This can be used to describe what the port is used for, To configure a port description:

1. Click **Configuration > Port > Port Description**.
2. Enter some text in the **Description** field.
3. Click **Apply**.

Parameter description

- **Port:**

This field shows the port number for this row.

- **Description:**

Use this field to configure a user-defined label for the port.

7.2.3 Traffic Overview

Use the **Traffic Overview** sub-menu to see the traffic statistics for all switch ports.

To show port statistics:

1. Click **Configuration > Port > Traffic Overview**.
2. Click a port number to show detailed statistics for that port.

Parameter description

- **Port:**

This field shows the port number for this row.

- **Packets:**

These fields shows the number of received and transmitted packets per port.

- **Bytes:**

These fields show the number of received and transmitted bytes per port.

- **Errors:**

These fields show the number of frames received in error and the number of incomplete transmissions per port.

- **Drops:**

These fields show the number of frames discarded due to ingress or egress congestion.

- **Filtered:**

This field shows the number of received frames filtered by the switch forwarding process.

7.2.4 Detailed Statistics

Use the **Detailed Statistics** sub-menu to see per-port traffic statistics.

To show detailed statistics:

1. Click **Configuration > Port > Detailed Statistics**.
2. Select the port number from the **Port Index** drop-down box to show detailed port statistics for that port.

Parameter description

Receive Total and Transmit Total

- **Rx and Tx Packets:**

These fields show the number of received and transmitted (good and bad) packets.

- **Rx and Tx Octets:**

These fields show the number of received and transmitted (good and bad) byte. This includes the FCS, but excludes framing bits.

- **Rx and Tx Unicast:**

These fields show the number of received and transmitted (good and bad) unicast packets.

- **Rx and Tx Multicast:**

These fields show the number of received and transmitted (good and bad) multicast packets.

- **Rx and Tx Broadcast:**

These fields show the number of received and transmitted (good and bad) broadcast packets.

- **Rx and Tx Pause:**

These fields show the number of received and transmitted pause frames.

Receive and Transmit Size Counters

These fields show the number of received and transmitted (good and bad) packets categorized by size.

Receive and Transmit Queue Counters

These fields show the number of received and transmitted packets per input and output queue.

Receive Error Counters

- **Rx Drops:**
This field shows the number of frames dropped due to ingress or egress congestion.
- **Rx CRC/Alignment:**
This field shows the number of frames received with CRC or alignment errors.
- **Rx Undersize:**
This field shows the number of frames smaller than 64 bytes received with valid CRCs.
- **Rx Oversize:**
This field shows the number of frames bigger than the configured maximum frame size received with valid CRCs.
- **Rx Fragments:**
This field shows the number of frames smaller than 64 bytes received with invalid CRCs.
- **Rx Jabber:**
This field shows the number of frames bigger than the configured maximum frame size received with invalid CRCs.
- **Rx Filtered:**
This field shows the number of received frames filtered by the forwarding process.

Transmit Error Counters

- **Tx Drops:**
This field shows the number of frames dropped due to output buffer congestion.
- **Tx Late/Exc. Coll.:**
This field shows the number of frames dropped due to excessive or late collisions.

7.2.5 QoS Statistics

Use the **QoS Statistics** sub-menu to see the queue statistics for all switch ports.

To show QoS statistics:

1. Click **Configuration > Port > QoS Statistics**.
2. Click a port number to show detailed statistics for that port.

Parameter description

- **Port:**

This field shows the port number for this row.

- **Rx/Tx:**

These fields show the number of received and transmitted packets per queue. Qn is queue number n, where n is 0 to 7 and Q0 is the highest priority queue.

7.2.6 SFP Information

Use the **SFP Information** sub-menu to see per-port information about SFP modules.

To show SFP information:

1. Click **Configuration > Port > SFP Information**.
2. Select the port number from the Port Index drop-down box to show detailed information about that port.

Parameter description

- **Connector Type:**

This field shows the connector type (e.g. UTP, SC, ST, LC).

- **Fiber Type:**

This field shows the fiber mode (Multi-Mode or Single-Mode).

- **Tx Central Wavelength:**

This field shows the fiber optic transmission central wavelength (e.g. 850nm, 1310nm, 1550nm).

- **Baud Rate:**

This field shows the maximum baud rate of the fiber module supported (e.g. 10M, 100M, 1G).

- **Vendor OUI:**

This field shows the manufacturer's OUI which is assigned by IEEE.

- **Vendor Name:**

This field shows the manufacturer's company name.

- **Vendor P/N:**

This field shows the product name.

- **Vendor Rev (Revision):**

This field shows the module revision.

- **Vendor SN (Serial Number):**

This field shows the manufacturer's serial number.

- **Date Code:**

This field shows the date this SFP module was made.

- **Temperature:**

This field shows the current temperature of SFP module.

- **Vcc:**

This field shows the working DC voltage of SFP module.

- **Mon1(Bias) mA:**

This field shows the bias current of SFP module.

- **Mon2(TX PWR):**

This field shows the transmit power of SFP module.

- **Mon3(RX PWR):**

This field shows the receiver power of SFP module.

7.3 ACL

Use the **ACL** sub-menu to configure the static ACL, get an overview of the status of all ACLs used across the device and configure rate limiters. ACLs are used to select traffic to be analyzed, forwarded, or influenced in some way. An ACL consists of one or more ACEs (ACL Entries). An ACE can match ports and policies. If an ACE is configured to match one or more policies, a single ACE can match any ports that are configured with a matching policy number. This means an ACE can be written once and used in more than one policy; and a policy can be defined once and used on many ports.

7.3.1 Ports

Use the **Ports** sub-menu to apply a policy and default ACL actions to each port. Default ACL actions affect frames received on a port unless the frame matches a specific ACE.

To configure ACL port actions and policies:

1. Click **Configuration > ACL > Ports**.
2. Configure the parameters for one or more ports.
3. Click **Save**.

Parameter description

- **Port:**

This field shows the port number for this row.

- **Policy ID:**

Use this field to configure the policy to apply to this port. The allowed values are 0 through 255. The default value is 0 which means no policy is applied.

- **Action:**

Use this drop-down box to **Permit** (default) or **Deny** forwarding of traffic.

- **Rate Limiter ID:**

Use this drop-down box to apply a rate limiter ID if the ACE matches. Choose **Disabled** not to apply a rate limiter or choose **1 to 16** to apply a rate limiter.

- **Port Copy:**

Use this drop-down box to apply copy traffic to another port if the ACE matches. Choose **Disabled** not to copy traffic or choose a port number to copy traffic.

- **Logging:**

Use this drop-down box to log traffic in the system log. Choose **Disabled** to disable this action or choose **Enabled** to log traffic.

Note:

The system log memory and logging rate is limited.

- **Shutdown:**

Use this drop-down box to shut down the port if any traffic is received. Choose **Disabled** to disable this action or choose **Enabled** to shut down port(s).

- **Counter:**

This field shows the number of frames that have triggered the default ACL action.

7.3.2 Rate Limiters

Use the **Rate Limiters** sub-menu to configure the rate limiters used by ACEs.

To configure ACL rate limiters:

1. Click **Configuration > ACL > Rate Limiter**.
2. Configure the **Rate** field for one or more rate limiters.
3. Click **Save**.

Parameter description

- **Rate Limiter ID:**

This field shows the rate limiter ID number for this row.

- **Rate:**

Use this field to configure a rate limit of 0 to 131071 packets per second.

7.3.3 Access Control List

Use the **Access Control List** sub-menu to define static ACLs.

An ACL is made of up to 256 ACEs. An ACE is a set of conditions that must match ingress traffic to trigger one or more actions. Evaluation of ACEs ends with the first matching ACE. If no ACE matches, the default ACL action configured on the ingress port is triggered.

To configure the Access Control List:

1. Click **Configuration > ACL > Access Control List**.
2. Click one of the following icons to view, add or edit an ACE:

 : Inserts a new ACE before the current row.

 : Edits the ACE row.

 : Moves the ACE up the list.

 : Moves the ACE down the list.

 : Deletes the ACE.

 : The lowest plus sign adds a new entry at the bottom of the ACE listings.

3. Configure the ACE parameters.
4. Click **Save**.

Parameter description

ACE parameters consist of conditions that must match to trigger an ACE and the actions that are carried out when an ACE is triggered.

ACE Conditions

The items shown on the **ACE Configuration** page depend on the conditions selected. E.g. select a **Frame Type** of **Ethernet Type** and the **Ethernet Type Parameters** item appears. The items that don't change are as follows.

- **Ingress Port:**

Use this drop-down box to configure the ingress port that matches this ACE. Choose **All** to match any port or choose a port number.

- **Policy Filter:**

Use this drop-down box to configure which policies match this ACE. Choose **Any** to configure this ACE to ignore the policy or choose **Specific** and then complete the **Policy Value** and **Policy Bitmask** fields to match specific policies that.

- **Frame Type:**

Use this drop-down box to configure which Ethernet frame type matches this ACE. Possible values are:

- **Any:** The ACE matches any frame type.
- **Ethernet Type:** The ACE matches Ethernet frames that are not IP or ARP frames. **Ethernet Type Parameters** appears when this is chosen.
- **ARP:** The ACE matches ARP/RARP frames.
- **IPv4:** The ACE matches any IPv4 packets.

MAC Parameters

- **SMAC Filter:**

This option appears when the **Frame Type** is **Ethernet Type** or **ARP**. Use this drop-down box to configure which source MAC addresses match this ACE. Choose **Any** to configure this ACE to ignore the source MAC address or choose **Specific** and then complete the **SMAC Value** field to match a specific source MAC address.

- **DMAC Filter:**

Use this drop-down box to configure which destination MAC address match this ACE. Possible values are:

- **Any:** The ACE matches any address.
- **MC:** The ACE matches multicast addresses.
- **BC:** The ACE matches broadcast addresses.
- **UC:** The ACE matches any unicast address.
- **Specific:** This option is available when the **Frame Type** is **Ethernet Type**. Choose this option and then complete **DMAC Value** field to match a specific destination MAC address.

VLAN Parameters

- **VLAN ID Filter:**

Use this drop-down box to configure which VLAN ID matches this ACE. Choose **Any** to configure this ACE to ignore the VLAN ID or choose **Specific** and then complete the **VLAN ID** field match a specific VLAN ID.

- **Tag Priority:**

Use this drop-down box to configure which tag priority matches this ACE. Choose **Any** to configure this ACE to ignore the tag priority or choose a tag priority from **0** to **7**.

Ethernet Type Parameters

- **EtherType Filter:**

Use this drop-down box to configure which Ethernet Length/Type field values match this ACE. Choose **Any** to configure this ACE to match frames with an Ethernet Length/Type field of 0x0600 to 0xFFFF excluding 0x0800 (IPv4), 0x0806 (ARP) and 0x86DD (IPv6). Choose **Specific** and then complete the **Ethernet Type Value** field to match a specific Ethernet Length/Type. Ethernet Type Values less than 0x0600 or equal to 0x0800 (IPv4), 0x0806 (ARP) or 0x86DD (IPv6) cannot be configured.

ARP Parameters

- **ARP/RARP and Request/Reply:**

Use a combination of these two drop-down boxes to configure which ARP opcode field values match this ACE. Possible combinations are:

- **Any; Any:** The ACE matches any ARP opcode.
- **Any; Request:** The ACE matches ARP (opcode 1) and RARP (opcode 3) requests.
- **Any; Reply:** The ACE matches ARP (opcode 2) and RARP (opcode 4) replies.
- **ARP; Any:** The ACE matches ARP requests (opcode 1) and replies (opcode 2).
- **ARP; Request:** The ACE matches ARP (opcode 1) requests.
- **ARP; Reply:** The ACE matches ARP (opcode 2) replies.
- **RARP; Any:** The ACE matches RARP requests (opcode 3) and replies (opcode 4).
- **RARP; Request:** The ACE matches RARP requests (opcode 3).
- **RARP; Reply:** The ACE matches RARP replies (opcode 4).
- **Other; Any:** The ACE matches non-ARP/RARP requests and replies (not opcode 1, 2, 3 or 4).
- **Other; Request:** The ACE matches non-ARP/RARP requests (not opcode 1, 2, 3 or 4).
- **Other; Reply:** The ACE matches non-ARP/RARP replies (not opcode 1, 2, 3 or 4).

- **Sender IP Filter and Target IP Filter:**

Use these drop-down boxes to configure which sender protocol address and target protocol address field values match this ACE. Choose **Any** to configure this ACE to ignore the sender/target protocol address field. Choose **Host** and then complete the **Sender IP Address** or **Target IP Address** field to match a specific sender or target protocol address. Choose **Network** and then complete the **Sender IP Address** or **Target IP Address** and **Sender IP Mask** or **Target IP Mask** fields to match all sender/target protocol addresses within a network.

- **ARP SMAC Match**

Use this drop-down box to configure the ACE to compare the sender hardware address in the ARP header against the source Ethernet address in the Ethernet frame's header. Choose **Any** to configure this ACE to ignore the comparison. Choose **0** to register a match in the ACE if the addresses are not equal or choose **1** to register a match in the ACE if the addresses are equal.

- **RARP DMAC Match**

Use this drop-down box to configure the ACE to compare the target hardware address in the RARP header against the destination Ethernet address in the Ethernet frame's header. Choose **Any** to configure this ACE to ignore the comparison. Choose **0** to register a match in the ACE if the addresses are not equal or choose **1** to register a match in the ACE if the addresses are equal.

- **IP/Ethernet Length**

Use this drop-down box to configure the ACE to check if the hardware address length is 6 bytes (Ethernet MAC address length) and the protocol address length is 4 bytes (IPv4 address length). Choose **Any** to configure this ACE to ignore the check. Choose **0** to register a match in the ACE if the check is not successful or choose **1** to register a match in the ACE if the check is successful.

- **IP**

Use this drop-down box to configure the ACE to check if the hardware address space in ARP/RARP frames is Ethernet. Choose **Any** to configure this ACE to ignore the check. Choose **0** to register a match in the ACE if the check is not successful or choose **1** to register a match in the ACE if the check is successful.

- **Ethernet**

Use this drop-down box to configure the ACE to check if the protocol address space in ARP/RARP frames is 0x800 (IPv4). Choose **Any** to configure this ACE to ignore the check. Choose **0** to register a match in the ACE if the check is not successful or choose **1** to register a match in the ACE if the check is successful.

IP Parameters

- **IP Protocol Filter**

Use this drop-down box to configure which protocol in the IP header matches this ACE. Choose **Any** to configure this ACE to ignore the protocol. Choose **ICMP**, **UDP** or **TCP** or choose **Other** and then complete the **IP Protocol Value** field match another protocol.

- **IP TTL**

Use this drop-down box to configure which IP time to live matches this ACE. Choose **Any** to configure this ACE to ignore the IP TTL, choose **Zero** to match a TTL of 0 or **Non-zero** to match a TTL of greater than 0.

- **IP Fragment**

Use this drop-down box to configure the ACE to check if the IP datagram is fragmented (IP more fragments flag is set or IP fragment offset field is more than 0). Choose **Any** to configure this ACE to ignore the check. Choose **Yes** to register a match in the ACE if the datagram is fragmented or choose **No** to register a match in the ACE if the datagram is unfragmented.

- **IP Option**

Use this drop-down box to configure the ACE to check if the IP datagram has options. Choose **Any** to configure this ACE to ignore the check. Choose **Yes** to register a match in the ACE if the datagram has options or choose **No** to register a match in the ACE if the datagram doesn't have options.

- **SIP Filter and DIP Filter**

Use these drop-down boxes to configure which source IP address and destination IP address field values match this ACE. Choose **Any** to configure this ACE to ignore the source/destination IP address field. Choose **Host** and then complete the **SIP Address** or **DIP Address** field to match a specific source or destination IP address. Choose **Network** and then complete the **SIP Address** or **DIP Address** and **SIP Mask** or **DIP Mask** fields to match all source/destination IP addresses within a network.

ICMP Parameters

- **ICMP Type Filter and ICMP Code Filter**

Use these drop-down boxes to configure which ICMP type and ICMP code field values match this ACE. Choose **Any** to configure this ACE to ignore the type/code field. Choose **Specific** and then complete the **ICMP Type Value** or **ICMP Code Value** field to match a specific type or code.

UDP Parameters

- **Source Port Filter and Dest. Port Filter**

Use these drop-down boxes to configure which UDP source port and UDP destination port field values match this ACE. Choose **Any** to configure this ACE to ignore the source/destination port field. Choose **Specific** and then complete the **Source Port No.** or **Dest. Port No.** field to match a specific source or destination port. Choose **Range** and then complete the **Source Port Range** or **Dest. Port Range** field to match a range of source or destination ports.

TCP Parameters

- **Source Port Filter and Dest. Port Filter**

Use these drop-down boxes to configure which TCP source port and TCP destination port field values match this ACE. Choose **Any** to configure this ACE to ignore the source/destination port field. Choose **Specific** and then complete the **Source Port No.** or **Dest. Port No.** field to match a specific source or destination port. Choose **Range** and then complete the **Source Port Range** or **Dest. Port Range** field to match a range of source or destination ports.

- **TCP FIN, TCP SYN, TCP RST, TCP PSH, TCP ACK and TCP URG**

Use these drop-down boxes to configure the ACE to check if the FIN (finish), SYN (synchronize), reset (RST), push (PSH), acknowledge (ACK) and urgent (URG) TCP control flags are set. Choose **Any** to configure this ACE to ignore the check. Choose **0** to fail the ACE if the flag is set or choose **1** to register a match in the ACE if the flag is set.

ACE Actions

- **Action:**

Use this drop-down box to **Permit** (default) or **Deny** forwarding of traffic that matches the ACE.

- **Rate Limiter:**

Use this drop-down box to apply a rate limiter ID if the ACE matches. Choose **Disabled** to disable this action or choose **1** to **16** to apply a rate limiter.

- **Port Copy:**

Use this drop-down box to apply copy traffic to another port if the ACE matches. Choose **Disabled** to disable this action or choose a port number to copy traffic.

- **Logging:**

Use this drop-down box to log traffic in the system log if the ACE matches. Choose **Disabled** to disable this action or choose **Enabled** to log traffic.

Note:

The system log memory and logging rate is limited.

- **Shutdown:**

Use this drop-down box to shutdown the ingress port(s) if the ACE matches. Choose **Disabled** to disable this action or choose **Enabled** to shutdown port(s).

- **Counter:**

This field shows the number of frames that have matched the ACE.

7.3.4 ACL Status

Use the **ACL Status** sub-menu to get an overview of the status of all ACEs used across the device.

To show the ACL status:

1. Click **Configuration > ACL > ACL Status**.
2. Select the part of the device that uses this ACL from the ACL User drop-down box.

Parameter description

- **User:**

This field shows the ACE user.

- **Ingress Port:**

This field shows the ingress port that matches this ACE. **All** means any port.

- **Frame Type:**

This field shows which Ethernet frame type matches this ACE. Possible values are:

- **Any:** The ACE matches any frame type.
- **EType:** The ACE matches Ethernet frames that are not IP or ARP frames.
- **ARP:** The ACE matches ARP/RARP frames.
- **IPv4:** The ACE matches IPv4 packets.
- **IPv4/ICMP:** The ACE matches ICMP packets.
- **IPv4/UDP:** The ACE matches UDP packets.
- **IPv4/TCP:** The ACE matches TCP packets.
- **IPv4/Other n:** The ACE matches IPv4 packets with protocol number n in the IP header.

- **Action:**

This field shows whether the ACE is configured to **Permit** or **Deny** forwarding matching traffic.

- **Rate Limiter:**

This field shows how the rate limiter ID is configured in the ACE. **Disabled** means the action is disabled.

■ **Port Copy:**

This field shows how the port copy action is configured in the ACE. **Disabled** means the action is disabled.

■ **CPU:**

This field shows whether the ACE is configured to forward frames that match the ACE to the CPU.

■ **CPU Once:**

This field shows whether the ACE is configured to forward the first frame that match the ACE to the CPU.

■ **Counter:**

This field shows the number of frames that have matched the ACE.

■ **Conflict:**

This field shows whether the ACE has not been applied to the hardware due to hardware limitations.

7.4 Aggregation

Use the **Aggregation** sub-menu to configure several ports as a trunk. A trunk is a logical port with the aggregate bandwidth of its component ports.

7.4.1 Static Trunk

Use the **Static Trunk** sub-menu to manually assign ports to static trunk.

The advantage of static trunks is that their ports immediately become members of the trunk without handshaking with their peer port. The disadvantage is that the peer device must be configured separately with the same settings or the trunk will not be established.

To configure a static trunk:

1. Click **Configuration > Aggregation > Static Trunk**.
2. Configure the **Hash Code Contributors**.
3. Click the corresponding radio button for each port you want to add to a trunk.

Note:

Each port in a trunk must be full duplex with the same speed.

4. Click **Save**.

Parameter description

Static trunk parameters consist of those that define member ports (**Aggregation Group Configuration**) and those that define how the traffic flows when the trunk is established (**Aggregation Mode Configuration**).

Aggregation Mode Configuration

This section consists of **Hash Code Contributors** that determine how traffic is divided amongst the member ports of established trunks.

- **Source MAC Address:**

Use this check box to add the source MAC address to the hash.

- **Destination MAC Address:**

Use this check box to add the destination MAC address to the hash.

- **IP Address:**

Use this check box to add the least significant byte of source and destination IP addresses to the hash.

- **TCP/UDP Port Number:**

Use this check box to add the least significant byte of source and destination TCP/UDP port numbers to the hash.

Aggregation Group Configuration

- **Group ID:**

This field shows the trunk's group ID for this row. **Normal** means no aggregation.

- **Port Members:**

Use these radio buttons to configure which trunk a port belongs to.

Note:

Each port in a trunk must be full duplex with the same speed.

7.4.2 LACP

Use the LACP sub-menu to define trunks that dynamically configure themselves.

Configuration

Use the **Configuration** sub-menu to configure LACP port members and how they negotiate to form trunks.

To configure LACP trunks:

1. Click **Configuration > Aggregation > LACP > Configuration**.
2. Configure the LACP trunk parameters.
3. Click **Save**.

Parameter description

- **Port:**

This field shows the port number for this row.

- **LACP Enabled:**

Use this check box to enable or disable LACP on this switch port. LACP will form a trunk when two or more ports are connected to the same partner. LACP can form maximum of twelve trunks.

- **Key:**

Use this drop-down box and field to configure a key for the trunk. Ports must have the same key to participate in a trunk. Choose **Auto** from the drop-down box to let the switch configure the key according to link speed (1 for 10Mb, 2 for 100Mb and 3 for 1Gb). Choose **Specific** and then complete the adjacent field to manually configure a key from 1 to 65535.

- **Role:**

Use this drop-down box to configure whether the port only responds to LACP packets (**Passive**) or sends LACP packets every second without waiting to receive them first (**Active**).

System Status

Use the **System Status** sub-menu to show the status of all LACP instances.

To show the LACP System status, click **Configuration > Aggregation > LACP > System Status**.

Parameter description

- **Aggr ID:**
This field shows the Aggregation ID associated with this aggregation instance.
- **Partner System ID:**
This field shows the system ID (MAC address) of the aggregation partner.
- **Partner Key:**
This field shows the Key that the partner has assigned to this aggregation ID.
- **Last changed:**
This field shows the time since this aggregation changed.
- **Local Ports:**
This field shows which ports are members of this aggregation on this switch.

Port Status

Use the **Port Status** sub-menu to show the status of all LACP instances, ordered by port.

To show the LACP Port status, click **Configuration > Aggregation > LACP > Port Status**.

Parameter description

- **Port:**

This field shows the port number for this row.

- **LACP:**

This field shows how LACP is configured on this port. Yes means that LACP is enabled and the port link is up. No means that LACP is not enabled or that the port link is down. Backup means that the port could not join the aggregation group but will join if another port leaves.

- **Key:**

This field shows the key assigned to this port. Only ports with the same key can aggregate together.

- **Aggr ID:**

This field shows the Aggregation ID assigned to this aggregation group.

- **Partner System ID:**

This field shows the partner's System ID (MAC address).

- **Partner Port:**

This field shows the partner port number connected to this port.

Port Statistics

Use the **Port Statistics** sub-menu to show counts of the LACP frames received, transmitted and discarded.

To show the LACP Port status, click **Configuration > Aggregation > LACP > Port Statistics**.

Parameter description

- **Port:**

This field shows the port number for this row.

- **LACP Received:**

This field shows how many LACP frames have been received at each port.

- **LACP Transmitted:**

This field shows how many LACP frames have been sent from each port.

- **Discarded:**

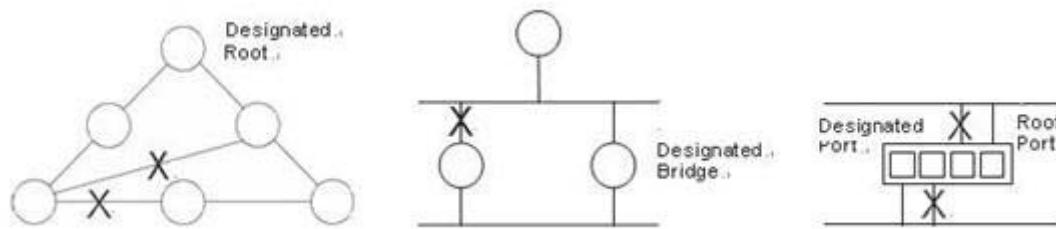
This field shows how many unknown or illegal LACP frames have been discarded at each port.

7.5 Spanning Tree

Use the Spanning Tree sub-menu to configure STP, RSTP and MSTP.

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, STP enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.



Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

7.5.1 Bridge Settings

Use the **Bridge Settings** sub-menu to configure STP system settings used by all STP Bridge instances on the switch.

To configure Bridge Settings:

1. Click **Configuration > Spanning Tree > Bridge Settings**.
2. Configure the STP bridge parameters.
3. Click **Save**.

Parameter description

STP bridge configuration parameters consist basic settings that configure STP and advanced settings that prevent leakage of network topology data and protect ports from connection to unauthorized switches.

Basic Settings

- **Protocol Version:**

Use this drop-down box to configure whether STP, RSTP or MSTP runs on this switch.

- **Bridge Priority:**

Use this drop-down box to configure the priority. Lower values mean higher priority. The bridge priority plus the MSTI instance number, concatenated with the MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST, otherwise this is the priority of the STP/RSTP bridge.

- **Forward Delay:**

Use this field to configure the delay used by STP Bridges to transit Root and Designated Ports to the Forwarding state (STP only). Valid values are from 4 to 30 seconds.

- **Max Age:**

Use this field to configure the maximum age of the information transmitted by the bridge when it is the Root Bridge. **MaxAge** must be between 6 and 40 seconds and must not be more than (**Forward Delay** - 1) * 2.

- **Maximum Hop Count:**

Use this field to configure the initial value of remaining hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are from 6 to 40 hops.

- **Transmit Hold Count:**

Use this field to configure the number of BPDUs a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are from 1 to 10 BPDUs per second.

Advanced Settings

- **Edge Port BPDU Filtering:**

Use this check box to configure whether a port explicitly configured as Edge will transmit and receive BPDUs.

- **Edge Port BPDU Guard:**

Use this check box to configure whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. Disabled ports enter the error-disabled state and are removed from the active topology.

- **Port Error Recovery:**

Use this check box to configure whether a port in the error-disabled state will be automatically enabled after the **Port Error Recovery Timeout**. If recovery is disabled, ports have to be manually disabled and then re-enabled for normal STP operation. The error-disabled state is also cleared by a system reboot.

- **Port Error Recovery Timeout:**

Use this check box to configure the time that must pass before a port in the error-disabled state is automatically re-enabled. Valid values are between 30 and 86400 seconds (24 hours).

7.5.2 MSTI Mapping

Use the **MSTI Mapping** sub-menu to configure the mapping between VLANs and each MSTI. The CIST automatically receives the VLANs not explicitly mapped.

To configure MSTI mapping:

1. Click **Configuration > Spanning Tree > MSTI Mapping**.
2. Configure the **MSTI Configuration** parameters.
3. Click **Save**.

Parameter description

MSTI Mapping parameters consist of **Configuration Identification** settings that label the collection of MSTI mappings and **MSTI Mapping** settings that contain the mappings themselves.

Configuration Identification

- **Configuration Name:**

Use this field to configure the name identifying the collection of VLAN to MSTI mappings. Bridges must share have the same **Configuration Name** and **Configuration Revision**, as well as the **MSTI Mapping** configuration to share spanning trees in an MSTI region. The name can be up to 32 characters.

- **Configuration Revision:**

Use this field to configure the revision of the MSTI configuration. This is between 0 and 65535.

MSTI Mapping

- **MSTI:**

This field shows the bridge instance.

- **VLANs Mapped:**

Use this field to configure a comma and/or a space separated list of VLANs mapped to the MSTI. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty (i.e. not having any VLANs mapped to it).

7.5.3 MSTI Priorities

Use the **MSTI Priorities** sub-menu to configure MSTI bridge instance priorities. The CIST is the default instance which is always active.

To configure MSTI Priorities:

1. Click **Configuration > Spanning Tree > MSTI Priorities**.
2. Configure the **Priority** for one or more bridge instances.
3. Click **Save**.

Parameter description

- **MSTI:**

This field shows the bridge instance.

- **Priority:**

Use this field to configure the bridge priority. Lower values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

7.5.4 CIST Ports

Use the **CIST Ports** sub-menu to configure the CIST on logically aggregated and physical ports.

To configure CIST Ports:

1. Click **Configuration > Spanning Tree > CIST Ports**.
2. Configure the parameters for one or more ports.
3. Click **Save**.

Parameter description

CIST port parameters consist of **CIST Aggregated Port Configuration** settings for logically aggregated ports and **CIST Normal Port Configuration** settings for physical ports, but the parameters are the same for both.

- **Port:**

This field shows the port number for this row.

- **STP Enabled:**

Use this check box to enable or disable STP on this switch port.

- **Path Cost**

Use this drop-down box to configure the cost incurred by this port when STP calculates the lowest path cost through this port to the root bridge. Choose **Auto** to automatically assign an 802.1D recommended patch cost or choose **Specific** and then complete the adjacent field to manually assign a value from 1 to 200000000.

- **Priority:**

Use this drop-down box to configure the priority of this port when STP must decide between identical path costs.

- **Admin Edge:**

Use this drop-down box to configure the state of the operEdge flag when the port is initialized. If the operEdge flag is true, the port transitions directly to the forwarding state because the port is at the edge of the network and an edge device (non-STP device) is attached to this port.

- **Auto Edge:**

Check this check box to enable automatic edge detection, so the operEdge flag is reset if a BPDU is received.

- **Restricted Role:**

Check this check box to prevent this port from becoming a Root Port. If this port has the best spanning tree priority vector, another port will become the Root Port and this port will become an Alternate Port. The restricted role can be used to prevent bridges outside the core region of the network from changing the spanning tree active topology in the core, possibly because non-core bridges are not under the full control of the administrator. This feature is also known as Root Guard.

Note:

The restricted role can cause a lack of spanning tree connectivity.

- **Restricted TCN:**

Check this check box to restrict propagation of received topology change notifications and topology changes to other ports. Restricted TCN can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. Restricted TCN is used to prevent bridges outside the core region of the network from causing address flushing in that region, possibly because non-core bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

- **BPDU Guard:**

Check this check box to make the port disable itself upon receiving a valid BPDU. This is independent of the port edge status. Disabled ports enter the error-disabled state and are removed from the active topology. A port in the error-disabled state is subject to the bridge Port Error Recovery configuration.

- **Point-to-point:**

Use this drop-down box to configure whether the port is connected to point-to-point or shared media. Choose **Forced True** for point-to-point media, choose **Forced False** for shared media or choose **Auto** to let the switch decide. Transition to the forwarding state is faster for point-to-point media.

7.5.5 MSTI Ports

Use the **MSTI Ports** sub-menu to configure MSTIs on logically aggregated and physical ports. An MSTI port is a virtual port that is instantiated for each active CIST and MSTI.

To configure MSTI Ports:

1. Click **Configuration > Spanning Tree > MSTI Ports**.
2. Choose an MSTI from the **Select MSTI** drop-down box and then click the **Get** button.
3. Configure the parameters for one or more ports.
4. Click **Save**.

Parameter description

MSTI port parameters consist of **MSTI Aggregated Port Configuration** settings for logically aggregated ports and **MSTI Normal Port Configuration** settings for physical ports, but the parameters are the same for both.

- **Port:**

This field shows the port number for this row.

- **Path Cost:**

Use this drop-down box to configure the cost incurred by this port when STP calculates the lowest path cost through this port to the root bridge. Choose **Auto** to automatically assign an 802.1D recommended patch cost or choose **Specific** and then complete the adjacent field to manually assign a value from 1 to 200000000.

- **Priority:**

Use this drop-down box to configure the priority of this port when STP must decide between identical path costs.

7.5.6 Bridge Status

Use the **Bridge Status** sub-menu to see an overview of all STP bridge instances.

To show Bridge Status:

1. Click **Configuration > Spanning Tree > Bridge Status**.
2. Click an item in the **MSTI** column to show the **STP Detailed Bridge Status** of that MSTI.

Parameter description

- **MSTI or Bridge Instance:**

This field shows the bridge instance. Click a bridge instance to show **STP Detailed Bridge Status**.

- **Bridge ID:**

This field shows the bridge ID of this bridge instance.

- **Root ID:**

This field shows the bridge ID of the root bridge.

- **Root Port:**

This field shows the switch port currently assigned the root port role.

- **Root Cost:**

This field shows the root path cost. For the root bridge it is zero. For all other bridges, it is the sum of the port path costs on the least cost path to the root bridge.

- **Regional Root**

This field shows the bridge ID of the regional root bridge in this bridge's MSTP region. (For the CIST instance only).

- **Internal Root Cost**

This field shows the regional root path cost. For the regional root bridge this is zero. For all other MSTP instances in the same MSTP region, it is the sum of the internal port path costs on the least cost path to the Internal Root Bridge. (For the CIST instance only).

- **Topology Flag:**

This field shows the current state of the topology change flag of this bridge instance.

- **Topology Change Count:**

This field shows the number of times the topology change flag has been set in the last second.

- **Topology Change Last:**

This field shows the time since last topology change occurred.

- **Port**

This field shows the logically aggregated or physical port number for this row.

- **Port ID**

This field shows the STP port ID that consists of the priority and the logical port index.

- **Role**

This field shows the STP port role. The port role can be **AlternatePort**, **BackupPort**, **RootPort** or **DesignatedPort**.

- **State**

This field shows the STP port state. The port state can be **Discarding**, **Learning** or **Forwarding**.

- **Path Cost**

This field shows the current STP port path cost.

- **Edge**

This field shows the state of the operEdge flag. If the operEdge flag is true, the port transitions directly to the forwarding state because the port is at the edge of the network and an edge device (non-STP device) is attached to this port.

- **Point2Point**

This field shows whether the port is connected to point-to-point or shared media. Transition to the forwarding state is faster for point-to-point media.

- **Uptime**

This field shows the time since the bridge port was last initialized.

7.5.7 Port Status

Use the **Port Status** sub-menu to show how CIST ports are participating in STP.

To show the STP port status, click **Configuration > Spanning Tree > Port Status**.

Parameter description

- **Port:**

This field shows the port number for this row.

- **CIST Role:**

This field shows the STP port role. The port role can be **AlternatePort**, **BackupPort**, **RootPort**, **DesignatedPort** or **Disabled**.

- **CIST State:**

This field shows the STP port state. The port state can be **Blocking**, **Learning** or **Forwarding**.

- **Uptime:**

This field shows the time since the bridge port was last initialized.

7.5.8 Port Statistics

Use the **Port Statistics** sub-menu to show the total number of BPDUs transmitted, received and discarded by each port. To show STP port statistics, click **Configuration > Spanning Tree > Port Statistics**.

Parameter description

- **Port:**

This field shows the port number for this row.

- **MSTP:**

This field shows the number of MSTP Configuration BPDUs received/transmitted on the port.

- **RSTP:**

This field shows the number of RSTP Configuration BPDUs received/transmitted on the port.

- **STP:**

This field shows the number of legacy STP Configuration BPDUs received/transmitted on the port.

- **TCN:**

This field shows the number of (legacy) Topology Change Notification BPDUs received/transmitted on the port.

- **Discarded Unknown:**

This field shows the number of unknown Spanning Tree BPDUs received and discarded on the port.

- **Discarded Illegal:**

This field shows the number of illegal Spanning Tree BPDUs received and discarded on the port.

7.6 MRSTP

7.6.1 Instances

Use the **Instances** sub-menu to configure Multiple Rapid Spanning Tree (MRSTP) system settings used by all MRSTP Bridge instances on the switch.

To configure MRSTP instances:

1. Click **Configuration > MRSTP > Instances**.
2. Configure the MRSTP bridge parameters or click an instance number to show the **MRSTP Instance Status** page.
3. Click **Save**.

Parameter description

MRSTP Instance Configuration

- **Global State:**

Use this drop-down box to enable or disable **MRSTP**.

- **Instance:**

This field shows the MRSTP bridge instance number. Click an instance number to show **MRSTP Instance Status**.

- **State:**

Use this check box to enable this MRSTP instance.

- **Version:**

Use this drop-down box to configure whether this instance uses **STP** or **RSTP**.

- **Priority:**

Use this drop-down box to configure the priority. Lower values mean higher priority. The bridge priority plus concatenated with the MAC address of the switch forms a Bridge Identifier.

- **Hello-Time:**

Use this drop-down box to configure the interval between periodic transmissions of STP Configuration Messages by designated ports when this is the root bridge. Valid values are in the range 1 to 10 seconds, and HelloTime must be $\leq (\text{MaxAge}/2)-1$.

- **Max-Age:**

Use this drop-down box to configure the maximum age of the information transmitted when this is the root bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be $\leq (\text{FwdDelay}-1)*2$.

- **FW-Delay:**

Use this drop-down box to configure the delay used by an MRSTP bridge instance to transit root and designated ports to the forwarding state (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

MRSTP Instance Status

- **Global State:**

This field shows whether MRSTP is globally enabled or disabled.

- **Instance State (Config.):**

This field shows whether this instance is configured as enabled or disabled.

- **Instance:**

This field shows the bridge instance number.

- **State:**

This field shows the operation state of this instance.

- **Bridge ID:**

This field shows the bridge ID of this bridge instance.

- **Bridge Priority**

This field shows the bridge priority of this bridge instance.

- **Root ID:**

This field shows the bridge ID of root bridge.

- **Root Priority**

This field shows the bridge priority of the root bridge.

- **Root Port**

This field shows the switch port currently assigned the root port role.

- **Root Path Cost**

This field shows the cost of the cheapest path to the root bridge (zero for the root bridge).

- **Current Max Age (sec)**

This field shows the max age time inherited from the root bridge.

- **Current Forward Delay (sec)**

This field shows forward delay time inherited from the root bridge.

- **Hello Time (sec)**

This field shows hello time inherited from the root bridge.

- **Topology Change Count**

This field shows the topology change count since this instance was operationally enabled.

- **Time Since Last Topology Change (sec)**

This field shows how long ago the topology changed.

7.6.2 Port Configuration

Use the **Port Configuration** sub-menu to configure the MRSTP port parameters.

To configure MRSTP ports:

1. Click **Configuration > MRSTP > Port Configuration**.
2. Configure the parameters for one or more ports.
3. Click **Save**.

Parameter description

- **Port:**

This field shows the port number for this row.

- **Instance**

Use this drop-down box to configure whether this port participates in MRSTP or not. Choose **None** or an MRSTP instance number.

- **Path Cost**

Use this drop-down box to configure the cost incurred by this port when MRSTP calculates the lowest path cost through this port to the root bridge. Choose **Auto** to automatically assign an 802.1D recommended path cost or choose **Specific** and then complete the adjacent field to manually assign a value from 1 to 200000000.

- **Priority:**

Use this drop-down box to configure the priority of this port when MRSTP must decide between identical path costs.

- **Admin Edge:**

Use this drop-down box to configure the state of the operEdge flag when the port is initialized. If the operEdge flag is true, the port transitions directly to the forwarding state because the port is at the edge of the network and an edge device (non-STP device) is attached to this port.

- **Admin P2P:**

Use this drop-down box to configure whether the port is connected to point-to-point or shared media. Choose **Forced True** for point-to-point media, choose **Forced False** for shared media or choose **Auto** to let the switch decide. Transition to the forwarding state is faster for point-to-point media.

- **Migrate Check**

Use this check box to force this port to send RSTP BPDUs instead of a legacy STP BPDUs. This enables a port to quickly get back to acting as an RSTP port.

7.6.3 Port Status

Use the **Port Status** sub-menu to show how ports are participating in MRSTP.

To show the MRSTP port status, click **Configuration > Spanning Tree > Port Status**.

Parameter description

- **Port:**

This field shows the port number for this row.

- **Instance**

This field shows whether this port participates in MRSTP or not. This is **None** or an MRSTP instance number.

- **State:**

This field shows the MRSTP port state. The port state can be **DISCARDING**, **LISTENING**, **FORWARDING**, **NON-MRSTP** or **INST-DSBL**. **INST-DSBL** means the bridge instance this port belongs to is disabled.

- **Role:**

This field shows the MRSTP port role. The port role can be **disable**, **alternate**, **backup**, **ROOT**, **DSGN** or **none**. This is **none** if the bridge instance the port belongs to is disabled or the port is not an MRSTP port or **DSGN** if this port is a designated port.

- **PathCost:**

This field shows the cost incurred by this port when MRSTP calculates the lowest path cost through this port to the root bridge. Choose **Auto** to automatically assign an 802.1D recommended patch cost or choose **Specific** and then complete the adjacent field to manually assign a value from 1 to 200000000.

- **PathCost Config.:**

This field shows the configured cost incurred by this port when MRSTP calculates the lowest path cost through this port to the root bridge. **Auto** means an 802.1D recommended patch cost is configured.

- **PathCost:**

This field shows the operational cost incurred by this port when MRSTP calculates the lowest path cost through this port to the root bridge.

- **Priority:**

This field shows the priority of this port when MRSTP must decide between identical path costs.

- **Admin Edge:**

This field shows the state of the operEdge flag when the port is initialized. If the operEdge flag is true, the port transitions directly to the forwarding state because the port is at the edge of the network and an edge device (non-STP device) is attached to this port.

- **Admin P2P:**

This field shows whether the port is configured as being connected to point-to-point or shared media. **Forced True** means point-to-point media, **Forced False** means shared media and **Auto** means the switch decides. Transition to the forwarding state is faster for point-to-point media.

7.7 IGMP and MLD Snooping

Use the **IGMP Snooping** and **MLD Snooping** sub-menus to configure selective forwarding of IPv4 and IPv6 multicast packets.

Without snooping, the switch can't tell which ports have multicast listeners connected to them, so the switch floods multicast packets to all ports. Each multicast listener must send a join packet to the local multicast router to receive multicast data via the router. The switch snoops on these join packets to build a table associating multicast destination addresses with destination ports, so each multicast packet can be selectively forwarded only to those ports associated with its destination multicast address. This saves bandwidth on the switch and processor power on non-member hosts. The switch can also use this table to function as an IGMP/MLD proxy, so only the first member to join and the last member to leave a multicast group trigger join and leave packets toward the multicast router. This saves memory and processing power on the router because it only has to process one join or leave packet.

7.7.1 Basic Configuration

Use the **Basic Configuration** sub-menu to configure global and port-specific parameters for IGMP and MLD snooping.

To configure basic IGMP and MLD snooping parameters:

1. Click **Configuration > IGMP Snooping** or **MLD Snooping > Basic Configuration**.
2. Configure the IGMP or MLD parameters.
3. Click **Save**.

Parameter description

Basic configuration parameters consist of global and port-specific parameters for IGMP and MLD snooping.

IGMP or MLD Snooping Configuration

- **Snooping Enabled:**
Use this check box to globally enable or disable IGMP or MLD snooping.
- **Unregistered IPMCv4 or IPMCv6 Flooding Enabled:**

Use this check box to enable or disable flooding of packets with unknown destination IPv4 or IPv6 multicast addresses.

- **MLD or IGMP SSM Range:**

Use these fields to configure an SSM (Source-Specific Multicast) range.

- **Proxy Enabled:**

Use this check box to enable or disable the IGMP Proxy.

Port Related Configuration

- **Port:**

This field shows the port number for this row.

- **Router Port:**

Use this check box to configure whether this port leads towards the IGMP querier.

- **Fast Leave:**

Use this check box to enable or disable fast leave on this port.

- **Throttling:**

Use this drop-down box to enable or disable the limit on the number of multicast groups a switch port can belong to. Configure **Unlimited** to disable the limit or a value of **1** to **10** to restrict the number of groups to that value.

7.7.2 VLAN Configuration

Use the **VLAN Configuration** sub-menu to configure how IGMP and MLD snooping operate over each VLAN.

To configure how IGMP and MLD snooping operates over VLANs:

1. Click **Configuration > IGMP Snooping** or **MLD Snooping > VLAN Configuration**.
2. Check the **Snooping Enabled** check box to allow the remaining parameters to be configured.
3. Click **Save**.
4. Configure the remaining parameters.
5. Click **Save**.

Parameter description

- **VLAN ID:**

This field shows the VLAN ID for this row.

- **Snooping Enabled:**

Use this check box to enable or disable snooping on this VLAN. A maximum of 32 VLANs can be enabled.

- **IGMP Querier or MLD Querier:**

Use this check box to enable or disable IGMP or MLD queries to be forwarded to this VLAN.

- **Compatibility:**

Use this drop-down box to configure which version of IGMP or MLD is allowed on this VLAN. Choose **IGMP-Auto**, **Forced IGMPv1**, **Forced IGMPv2** or **Forced IGMPv3** for IGMP or choose **MLD-Auto**, **Forced MLDv1**, **Forced MLDv2** or **MLD-Auto** for MLD.

- **Rv:**

Use this field to configure the Robustness Variable to a value from 1 to 255 (default 2). The Robustness Variable allows tuning of the expected packet loss on a network.

- **QI:**

Use this field to configure the Query Interval to a value from 1 to 31744 (default 125) seconds. The Query Interval is the time between General Queries sent by the querier.

- **QRI:**

Use this field to configure the Query Response Interval to a value from 0 to 31744 (default 100) in tenths of a second. The Query Response Interval is the Max Response Time (IGMP) or Maximum Response Delay (MLD) used to calculate the value of the Max Resp Code (IGMP) or Maximum Response Code (MLD) field in periodic General Queries.

- **LLQI:**

Last Member Query Interval (LMQI) and Last Listener Query Interval (LLQI) are configuration items for IGMP (IPv4) and MLD (IPv6) respectively. They are equivalent in purpose. Use this field to configure LMQI or LLQI to a value from 0 to 31744 (default 10) in tenths of a second. LMQI is the Max Response Time (IGMP) or Maximum Response Delay (MLD) used to calculate the value of the Max Resp Code (IGMP) or Maximum Response Code (MLD) field in Group-Specific Queries (IGMP) or Multicast Address Specific Queries (MLD) and Group-and-Source-Specific Queries (IGMP) or Multicast Address and Source Specific Queries.

- **URI:**

Use this field to configure the Unsolicited Report Interval to a value from 0 to 31744 (default 1) in seconds. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group.

7.7.3 Port Group Filtering

Use the **Port Group Filtering** sub-menu to filter multicast joins on a per-port basis. When a filter is configured for a multicast group, the port never gets multicast traffic from the upstream multicast router because multicast joins are dropped at the switch before the switch's IGMP/MLD Snooping process or the router can receive them.

For example, in metropolitan or multiple-dwelling unit installations each customer is connected to a port, so Port Group Filtering can be used to ensure the distribution of multicast services such as IPTV matches customer subscriptions.

To configure a port group filter:

1. Click **Configuration > IGMP Snooping** or **MLD Snooping > Port Group Filtering**.
2. Click **Add new Filtering Group**.
3. Configure the parameters.
4. Click **Save**.

Parameter description

- **Port:**

Use this drop-down box to configure which port will be filtered.

- **Filtering Groups:**

Use this field to configure which multicast group will be filtered.

7.7.4 Status

Use the **Status** sub-menu to show an overview of the status of IGMP or MLD Snooping.

To show IGMP or MLD snooping status, click **Configuration > IGMP Snooping** or **MLD Snooping > Status**.

Parameter description

- **VLAN ID:**

This field shows the VLAN ID for this row.

- **Querier Version:**

This field shows the version of the querier.

- **Host Version:**

This field shows the host version.

- **Querier Status:**

This field shows the status of the querier. Possible values are **ACTIVE**, **IDLE** or **DISABLE**. **DISABLE** means the interface is administratively disabled.

- **Queries Transmitted:**

This field shows the number of queries transmitted.

- **Queries Received:**

This field shows the number of queries received.

- **V1 Reports Received and V2 Reports Received:**

This field shows the number of version 1 and 2 reports received.

- **V3 Reports Received:**

This field shows the number of IGMP version 3 reports received.

- **V1 Leaves Received:**

This field shows the number of MLD version 1 leaves received.

- **V2 Leaves Received:**

This field shows the number of IGMP version 2 leaves received.

- **Port:**

This field shows which port will be filtered.

- **Filtering Groups:**

This field shows which ports lead towards the multicast router or IGMP querier. **Static** means this port is a router port. **Dynamic** means this port can learn to be a router port. **Both** means this port is statically configured and can learn to be a router port.

7.7.5 Group Information

Use the **Group Information** sub-menu to show where each multicast group member is connected.

To show group information, click **Configuration > IGMP Snooping or MLD Snooping > Group Information**.

Parameter description

- **VLAN ID:**

This field shows the VLAN ID for this row.

- **Groups:**

This field shows the multicast group address for this row.

- **Port Members:**

This field shows the ports that are connected to members of this group.

7.7.6 IPv4 and IPv6 SSM Information

Use the **IPv4 SSM Information** or **IPv6 SSM Information** sub-menu to see how Source-Filtered Multicasting is being used across the switch.

Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core network technology of IP multicast targeted for audio and video broadcast application environments.

For the SSM delivery mode, an IP multicast receiver host must use IGMPv3 or MLDv2 to subscribe to channel (S, G). By subscribing to this channel, the receiver host is indicating that it wants to receive IP multicast traffic sent by source host S to group G. The network will deliver IP multicast packets from source host S to group G to all hosts in the network that have subscribed to the channel (S, G).

SSM does not require group address allocation within the network, only within each source host. Different applications running on the same source host must use different SSM groups. Different applications running on different source hosts can arbitrarily reuse SSM group addresses without causing any excess traffic on the network.

IPv4 addresses in the range 232.0.0.0/8 (232.0.0.0 to 232.255.255.255) are reserved for SSM by IANA. In the switch, you can configure SSM for arbitrary IP multicast addresses also.

To show SSM Information, click **Configuration > IGMP Snooping** or **MLD Snooping > IPv4 SSM Information** or **IPv6 SSM Information**.

Parameter description

IGMPv3 Information Table Columns

- **VLAN ID:**

This field shows the VLAN ID for this row.

- **Group:**

This field shows the multicast group address for this row.

- **Port:**

This field shows the port number for this row.

- **Mode:**

This field shows the filtering mode maintained on a VLAN ID, port number, Group Address basis. It can be either **Include** or **Exclude**.

- **Source Address:**

This field shows the IP Address of the source. The switch can filter up to 128 IP source addresses.

- **Type:**

This field shows whether this multicast group is allowed on this VLAN/port.

7.8 MVR

Use the **MVR** (Multicast VLAN Registration) sub-menu to enable multicast listeners in one VLAN to join or leave multicast groups on another VLAN. For example in a multicast television application, content is multicasted to the multicast VLAN in the network core. Subscribers are connected to access switches at the network edge and belong to subscriber VLANs. Access switches are connected to the network core via their uplink ports. These uplink ports are called MVR source ports because they send and receive multicast data to and from the multicast VLAN. When a subscriber selects a TV channel, the access switch forwards the subscriber's IGMP join message to the multicast VLAN and begins selectively forwarding multicast content to the subscriber.

7.8.1 Configuration

Use the **Configuration** sub-menu to establish MVR over a VLAN on selected ports.

To configure MVR:

1. Click **Configuration > MVR > Configuration**.
2. Configure the parameters.
3. Click **Save**.

Parameter description

- **MVR Mode:**
Use this check box to globally enable or disable MVR.
- **VLAN ID:**
Use this field to configure the subscriber VLAN ID.
- **Port:**
This field shows the port number for this row.
- **Mode:**
Use this drop-down box to enable or disable MVR on this port.

- **Type:**

Use this drop-down box to configure whether this port is connected to a multicast source or a multicast receiver.

- **Immediate Leave:**

Use this drop-down box to enable or disable fast leave on this port.

7.8.2 Groups Information

Use the **Group Information** sub-menu to show where each MVR group member is connected.

To show MVR group information, click **Configuration > MVR > Groups Information**.

Parameter description

- **VLAN ID:**

This field shows the VLAN ID for this row.

- **Groups:**

This field shows the multicast group address for this row.

- **Port Members:**

This field shows the ports that are connected to members of this group.

7.8.3 Statistics

Use the **Statistics** sub-menu to show an overview of the status of MVR.

To show the MVR status, click **Configuration > MVR > Statistics**.

Parameter description

- **VLAN ID:**
This field shows the VLAN ID for this row.
- **V1 Reports Received, V2 Reports Received and V3 Reports Received:**
This field shows the number of IGMP version 1, 2 and 3 reports received.
- **V2 Leaves Received:**
This field shows the number of IGMP version 2 leaves received.

7.9 LLDP

Use the **LLDP** sub-menu to share information about the main capabilities of the switch with adjacent devices over the link layer. LLDP (Link Layer Discovery Protocol) is an 802.1ab standard that enables devices to exchange information such as management address, identity and how they connect to their neighbors. This information is stored in each device's MIB and can be accessed and collated by a centrally located network management system for presentation as a topology.

7.9.1 LLDP Configuration

Use the **LLDP Configuration** sub-menu to configure global LLDP timers and how LLDP works on a port-by-port basis.

To configure LLDP:

1. Click **Configuration > LLDP > LLDP Configuration**.
2. Configure the parameters.
3. Click **Save**.

Parameter description

- **Tx Interval:**

Use this field to configure how often this switch transmits LLDP frames to its neighbors. Valid values are from 5 to 32768 seconds.

- **Tx Hold:**

Use this field to configure the Time-To-Live (TTL) field in LLDP frames transmitted by this switch. The TTL determines how long the recipient considers the information it receives as valid. The TTL is Tx Hold multiplied by Tx Interval seconds. Valid values are from 2 to 10 times.

- **Tx Delay:**

Use this field to configure the minimum time this switch waits to inform neighbors of a configuration change. Valid values are from 1 to 8192 seconds but Tx Delay cannot be longer than 1/4 of Tx Interval.

- **Tx Reinit:**

Use this field to configure how long this switch waits to re-initialize a port after transmission of an LLDP shutdown frame. An LLDP shutdown frame is transmitted to neighboring units to indicate the LLDP information is invalid (e.g. because a port is disabled, LLDP is disabled or the switch is rebooted). Valid values are from 1 to 10 seconds.

- **Port:**

This field shows the port number for this row.

- **Mode:**

Use this drop-down box to configure whether the switch sends, receives or sends and receives LLDP frames. Possible values are:

- **Rx only:** The switch receives but doesn't transmit LLDP information.
- **Tx only:** The switch transmits but doesn't receive LLDP information.
- **Disabled:** The switch receives and transmits LLDP information.
- **Enabled:** The switch doesn't receive or transmit LLDP information.

- **CDP Aware:**

Use this check box to enable the switch to decode incoming CDP frames. The switch doesn't transmit CDP frames and CDP frames are only decoded if LLDP on the port is enabled. Only CDP TLVs that can be mapped to corresponding fields in the LLDP neighbors' table are decoded. All other TLVs are discarded (unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics). CDP TLVs are mapped to the LLDP neighbors' table as follows.

- The CDP Device ID is mapped to the LLDP Chassis ID.
- The CDP Address is mapped to the LLDP Management Address. The CDP Address can contain multiple addresses, but only the first address is shown in the LLDP neighbors' table.
- The CDP Port ID is mapped to the LLDP Port ID.
- The CDP Version and Platform TLV is mapped to the LLDP System Description TLV.

CDP and LLDP both support a system capabilities TLV, but CDP capabilities cover capabilities that are not part of LLDP. These capabilities are shown as *other* in the LLDP neighbors' table. If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch.

Note:

When CDP awareness on a port is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.

- **Port Descr, Sys Name, Sys Descr, Sys Capa and Mgmt Addr:**

Use these check boxes to configure whether port descriptions, the system name, the system description, system capabilities and management address are included in the LLDP information sent.

7.9.2 LLDP Neighbors

Use the LLDP Neighbors sub-menu to show an overview of LLDP neighbors.

To show LLDP neighbors, click **Configuration > LLDP > LLDP Neighbors**.

Parameter description

- **Local Port:**

This field shows the port on which the LLDP frame was received.

- **Chassis ID:**

This field shows the chassis ID of the neighbor.

- **Remote Port ID:**

This field shows the port ID of the neighbor port.

- **System Name:**

This field shows the system name of the neighbor.

- **Port Description:**

This field shows the port description of the neighbor port.

- **System Capabilities:**

This field shows what the neighboring device can do. The possible capabilities are **Other**, **Repeater**, **Bridge**, **WLAN Access Point**, **Router**, **Telephone**, **DOCSIS cable device**, **Station only** and **Reserved**. When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

- **System Description:**

This field shows the system description of the neighbor unit.

- **Management Address:**

This field shows the management address of the neighbor.

7.9.3 LLDP MED Configuration

Use the **LLDP MED Configuration** sub-menu to configure location information and quality of service settings for VoIP endpoint devices. Link Layer Discovery Protocol for Media Endpoint Discovery (LLDP-MED) is an ANSI-TIA-1057 standard that builds on LLDP to provide the following facilities:

- Auto-discovery of LAN policies for plug and play networking. VLAN ID, Layer 2 Priority and Differentiated services (DSCP) settings can be controlled by a policy.
- Device location discovery to allow creation of location databases and, in the case of VoIP, Enhanced 911 services.
- Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, serial or asset number).

To configure LLDP-MED:

1. Click **Configuration > LLDP > LLDP-MED Configuration**.
2. Configure the **Fast Start Repeat Count**, **Coordinates Location**, **Civic Address Location** and **Emergency Call Service** parameters.
3. Under **Policies**, click **Add new policy** and complete the policy configuration fields
4. Click **Save**. The **Policy Port Configuration** parameters appear.
5. Use the check boxes to enable these policies on a port-by-port basis.
6. Click **Save**.

Parameter description

Fast Start Repeat Count

Use the **Fast start repeat count** field to configure the number of times an LLDP-MED fast start frame is sent to mitigate the risk of frame loss. When an LLDP-MED device is detected, the switch temporarily increases the rate at which LLDP-MED frames are sent to one per second, so VoIP devices become available quickly in an emergency.

Coordinates Location

- **Latitude and Longitude:**

Use these fields and drop-down boxes to configure the number of degrees **North** or **South** of the equator and **East** or **West** of the prime meridian this switch is located. Latitude must be between 0 and 90 degrees and longitude must be between 0 and 180 degrees with a maximum of 4 digits.

- **Altitude:**

Use these fields and drop-down boxes to configure the altitude of the switch from -32767 to 32767 with a maximum of 4 digits. Choose **Meters** to configure a distance in meters from the vertical datum or choose **Floors** to configure a distance in floors from ground level outside the building or the level of the main entrance.

- **Map Datum:**

Use this drop-down box to configure one of the following Map Datums.

- **WGS84:** (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.
- **NAD83/NAVD88:** North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). Use this datum pair when referencing locations on land, not near tidal water.
- **NAD83/MLLW:** North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). Use this datum pair when referencing locations on water/sea/ocean.

Civic Address Location

Use these fields to configure IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

- **Country code:**

The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.

- **State:**

National subdivisions (state, canton, region, province, prefecture).

- **County:**

County, parish, gun (Japan), district.

- **City:**

City, township, shi (Japan) - Example: Copenhagen.

- **City district:**

City division, borough, city district, ward, chou (Japan).

- **Block (Neighborhood):**

Neighborhood, block.

- **Street:**

Street - Example: Poppelvej.

- **Leading street direction:**

Leading street direction - Example: N.

- **Trailing street suffix:**

Trailing street suffix - Example: SW.

- **Street suffix:**

Street suffix - Example: Ave, Platz.

- **House no.:**

House number - Example: 21.

- **House no. suffix:**

House number suffix - Example: A, 1/2.

- **Landmark:**

Landmark or vanity address - Example: Columbia University.

- **Additional location info:**

Additional location info - Example: South Wing.

- **Name:**

Name (residence and office occupant) - Example: Flemming Jahn.

- **Zip code:**

Postal/zip code - Example: 2791.

- **Building:**

Building (structure) - Example: Low Library.

- **Apartment:**
Unit (Apartment, suite) - Example: Apt 42.
- **Floor:**
Floor - Example: 4.
- **Room no.:**
Room number - Example: 450F.
- **Place type:**
Place type - Example: Office.
- **Postal community name:**
Postal community name - Example: Leonia.
- **P.O. Box:**
Post office box (P.O. BOX) - Example: 12345.
- **Additional code:**
Additional code - Example: 1320300003.
- **Emergency Call Service:**
Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.
Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services.

The policy attributes advertised are:

- Layer 2 VLAN ID
- Layer 2 IEEE 802.1Q user priority
- Layer 3 IETF RFC 2474 Differentiated Services Code Point (DSCP)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

- Voice
- Guest Voice
- Softphone Voice
- Video Conferencing
- Streaming Video
- Control / Signalling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

LLDP-MED is intended to run between this switch and endpoint devices, so it doesn't need to advertise the multitude of policies configured on interior aggregated links.

- **Policy ID:**

This field shows the automatically generated ID number for the policy.

- **Application Type:**

Use this drop-down box to configure the following application type associated with this policy.

- **Voice:** This is for dedicated IP phones. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolating them from data applications.
- **Voice Signalling:** This is for network topologies that separate voice media and signalling policies.
- **Guest Voice:** This supports a limited feature-set voice service for guests with their own IP phones.
- **Guest Voice Signalling:** This is for network topologies that separate guest voice media and signalling policies.

- **Softphone Voice:** This is for phones that are implemented as a software applications on a PC. This class of endpoints usually uses an untagged VLAN or a single tagged data VLAN. When a network policy is defined for use with an untagged VLAN, the L2 priority field is ignored and only the DSCP value has relevance.
- **Video Conferencing:** This is for dedicated appliances supporting real-time interactive video/audio services.
- **Streaming Video:** This is for broadcast or multicast based video content distribution applications that require specific network policy treatment. This application type doesn't cover video applications relying on TCP with buffering.
- **Video Signalling:** This is for network topologies that separate video media and signalling policies.
- **Tag:**
Use this drop-down box to configure an untagged or IEEE 802.1Q tagged VLAN for this policy. Choose **Untagged** to configure a policy not to include tag headers in frames sent by end devices. An untagged policy ignores the VLAN ID and Layer 2 priority fields. Choose **Tagged** to configure a policy to include tag headers in frames sent by end devices. A tagged policy uses the VLAN ID, Layer 2 priority and DSCP fields.
- **VLAN ID:**
Use this field to configure the VLAN ID for this policy.
- **L2 Priority:**
Use this field to configure an IEEE 802.1Q tag priority of **0** (default priority) to **7** for this policy.
- **DSCP:**
Use this field to configure an RFC 2474 differentiated services code point of **0** (default best-effort forwarding) to **63** for this policy.

Policy Port Configuration

This table of ports and policies appears after adding a policy.

- **Port:**
This field shows the port number for this row.
- **Policy Id:**
Use these check boxes to configure which policies apply to this port.

7.9.4 LLDP MED Neighbors

Use the **LLDP MED Neighbors** sub-menu to show an overview of all LLDP-MED neighbors.

To show LLDP-MED neighbors click **Configuration > LLDP > LLDP-MED Neighbors**.

Parameter description

- **Port:**

This field shows the port number on which the LLDP frame was received.

- **Device Type:**

LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.

LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

- a. LAN Switch/Router
- b. IEEE 802.1 Bridge
- c. IEEE 802.3 Repeater (included for historical reasons)
- d. IEEE 802.11 Wireless Access Point

e. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method

- **LLDP-MED Endpoint Device Definition:**

LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework.

Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.

Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

- **LLDP-MED Generic Endpoint (Class I):**

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

- **LLDP-MED Media Endpoint (Class II):**

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.

Discovery services defined in this class include media-type-specific network layer policy discovery.

- **LLDP-MED Communication Endpoint (Class III):**

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management.

- **LLDP-MED Capabilities:**

This field shows what the neighboring device can do. The possible capabilities are:

- **LLDP-MED capabilities**
- **Network Policy**
- **Location Identification**
- **Extended Power via MDI - PSE**
- **Extended Power via MDI - PD**
- **Inventory**

- **Application Type:**

This field shows the primary function of the neighboring device. The possible application types are:

- **Voice:** This is for dedicated IP phones. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolating them from data applications.
- **Voice Signalling:** This is for network topologies that separate voice media and signalling policies.
- **Guest Voice:** This supports a limited feature-set voice service for guests with their own IP phones.
- **Guest Voice Signalling:** This is for network topologies that separate guest voice media and signalling policies.
- **Softphone Voice:** This is for phones that are implemented as a software applications on a PC. This class of endpoints usually uses an untagged VLAN or a single tagged data VLAN. When a network policy is defined for use with an untagged VLAN, the L2 priority field is ignored and only the DSCP value has relevance.
- **Video Conferencing:** This is for dedicated appliances supporting real-time interactive video/audio services.
- **Streaming Video:** This is for broadcast or multicast based video content distribution applications that require specific network policy treatment. This application type doesn't cover video applications relying on TCP with buffering.
- **Video Signalling:** This is for network topologies that separate video media and signalling policies.

- **Policy:**

This field shows whether the policy is **Defined** or **Unknown**, and indicates whether the Endpoint Device wants to explicitly advertise that the policy is required by the device.

- **TAG:**

This field shows whether the specified application type is using a tagged or an untagged VLAN. The possible application types are:

- **Untagged:** The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q.
- **Tagged:** The device is using the IEEE 802.1Q tagged frame format.

- **VLAN ID:**

This field shows the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of **1** through **4094** is used to define a valid VLAN ID. A value of **0** (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

- **Priority:**

This field shows the IEEE 802.1Q tag priority of **0** (default priority) to **7** for this policy.

- **DSCP:**

This field shows an RFC 2474 differentiated services code point of **0** (default best-effort forwarding) to **63** for this policy.

7.9.5 Port Statistics

Use the **Port Statistics** sub-menu to show the total number of LLDP frames sent, received and discarded; unrecognized and discarded TLVs; and the number of entries that have changed in the neighbors table.

To show LLDP Statistics, click **Configuration > LLDP > Port Statistics** to show LLDP counters.

Parameter description

Global Counters

- **Neighbor entries were last changed at:**

This shows the absolute time when and elapsed time since the neighbors table last changed.

- **Total Neighbors Entries Added:**

This field shows the number of new entries added since switch reboot.

- **Total Neighbor Entries Deleted:**

This field shows the number of new entries deleted since switch reboot.

- **Total Neighbors Entries Dropped:**

This field shows the number of LLDP frames dropped due to the entry table being full.

- **Total Neighbors Entries Aged Out:**

This field shows the number of entries deleted due to the Time-To-Live expiring.

Local Counters

- **Local Port:**

This field shows the port on which LLDP frames are received or transmitted.

- **Tx Frames:**

This field shows the number of LLDP frames transmitted on the port.

- **Rx Frames:**

This field shows the number of LLDP frames received on the port.

- **Rx Errors:**

This field shows the number of received LLDP frames containing some kind of error.

- **Frames Discarded:**

This field shows the number of LLDP frames discarded because the there was not enough switch memory to hold another neighbor entry. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received or when the entry ages out.

- **TLVs Discarded:**

This field shows the number of LLDP frames with malformed TLV fields that have been discarded.

- **TLVs Unrecognized:**

This field shows the number of LLDP frames received with well-formed TLVs that have an unknown type.

- **Org. Discarded:**

This field shows the number of organizationally specific TLVs received and discarded.

- **Age-Outs:**

This field shows how many entries have been removed from the neighbor table because their Time-To-Live (TTL) has expired. Each LLDP frame contains a TTL TLV field. If no new LLDP frame is received within the TTL, the LLDP information is removed, and the Age-Outs counter is incremented.

7.10.1 Configuration

Use the **Configuration** sub-menu to set a time-out for dynamic entries in the CAM, define how each port can influence the CAM and set new static entries.

To configure MAC Address Table

1. Click **Configuration > Filtering Data Base > Configuration**.
2. Click **Add new static entry**.
3. Configure the parameters.
4. Click **Save**.

Parameter description

Aging Configuration

- **Disable Automatic Aging:**
Check this check box to configure the CAM never to remove an entry.
- **Aging Time:**
Use this field to configure a time-out between **10** and **1000000** (default **300**) seconds for CAM entries.

MAC Table Learning

Use the **MAC Table Learning** parameters to configure how the CAM is updated. If the learning mode for a given port is greyed out, another module is in control of how frames arriving on this port update the CAM. An example of such a module is the MAC-Based Authentication under 802.1X. Each port update the CAM (or learn new entries) based upon the following options.

- **Port Members**
These fields show the ports to be configured.
- **Auto:**
Check this radio button to ensure learning is done as soon as a frame with unknown source MAC address is received.

- **Disable:**

Check this radio button to disable learning from this port.

- **Secure:**

Check this check box to ensure only frames with a static entry in the CAM are switched.

Note:

Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration

Use the **Static MAC Table Configuration** parameters to configure up to 64 fixed entries in the CAM.

- **VLAN ID:**

Use this field to configure the VLAN ID of the entry.

- **MAC Address:**

Use this field to configure the MAC address of the entry.

- **Port Members:**

Use these check boxes to configure which ports are members of the entry.

7.10.2 Dynamic MAC Table

Use the **Dynamic MAC Table** sub-menu to show the state of the CAM.

To show the CAM, click **Configuration > Filtering Data Base > Dynamic MAC Table**.

Parameter description

MAC Table Columns

- **Type:**

This field shows whether the entry is a static or a dynamic entry.

- **VLAN:**

This field shows the VLAN ID of the entry.

- **MAC address:**

This field shows the MAC address of the entry.

- **Port Members:**

These check boxes show the ports that are members of the entry.

7.11 VLAN

Use the **VLAN** sub-menu to configure which ports can communicate with other ports.

7.11.1 VLAN Membership

Use the **VLAN Membership** sub-menu to add, delete or modify VLANs.

To configure VLAN membership:

1. Click **Configuration > VLAN > VLAN membership**.
2. Click **Add New VLAN**.
3. Configure the parameters.
4. Click **Save**.

Parameter description

- **VLAN ID:**

Use this field to configure the identity of this VLAN.

- **VLAN Name:**

Use this field to configure the name of VLAN. The VLAN name can only contain alphabetic or numeric characters and should contain at least one alphabetic character.

- **Port Members:**

Use these check boxes to configure membership for each VLAN ID. No ports are members by default.

7.11.2 Ports

Use the **Ports** sub-menu to configure ingress and egress VLAN tagging port behavior.

To configure VLAN ports:

1. Click **Configuration > VLAN > Ports**.
2. Configure the parameters.
3. Click **Save**.

Parameter description

- **Ethertype for Custom S-ports:**

Use this field to configure the ethertype used for custom service ports. This is a global setting for all the Custom S-ports. Custom ethertype enables the user to change the Ethertype value on a port to any value to support network devices that do not use the standard 0x8100 Ethertype field value on 802.1Q-tagged or 802.1p-tagged frames.

- **Port:**

This shows the logical port number of this row.

- **Port Type:**

Use this drop-down box to configure the port as **Unaware**, **C-port** (Customer port), **S-port** (Service port), **S-custom-port** (Custom Service port). If the port type is unaware, all frames are classified with the **PVID** and tags are not removed.

- **Ingress Filtering:**

Use this check box to enable or disable (default) ingress filtering on a port. There are two ingress filtering rules which can be applied to a port. Rule 1 forwards only frames with VIDs matching this VID of the port. Rule 2 drops untagged frames. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded.

- **Frame Type:**

Use this drop-down box to configure what kind of frames this port accepts. Choose **All** (default) to accept all frames, choose **Tagged** to accept only tagged frames or choose **Untagged** to accept only untagged frames.

- **Egress Rule:**

Use this drop-down box to configure how frames are tagged before they're sent. If **Trunk** is selected, the classified VLAN tag is inserted in frames transmitted on the port. This mode is for ports connected to VLAN aware switches. If **Hybrid** is selected and the classified VLAN ID of a frame transmitted on the port is different from the port VLAN ID, a tag with the classified VLAN ID is inserted in to the frame. If **Access** is selected, all frames are untagged before transmission.

- **PVID:**

Use this field to configure the port VLAN identifier (default 1).

Note:

The port must be a member of the same VLAN as the Port VLAN ID.

7.11.3 Switch Status

Use the **Switch Status** sub-menu to show the members of each VLAN classified by VLAN user.

To show VLAN membership status:

1. Click **Configuration > VLAN > Switch Status**.
2. Use the VLAN user drop-down box to select the specific VLAN user of the configuration or choose **Combined** to see all VLANs from any VLAN user.

Parameter description

- **VLAN User** (unlabelled drop-down box to the left of Auto-refresh):

A VLAN configuration can come from one of the following sources (users):

- **CLI/Web/SNMP**: These are referred to as **static** in the web interface.
- **NAS**: A Network Access Server (NAS) provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.
- **MVRP**: Multiple VLAN Registration Protocol (MVRP) allows dynamic registration and de-registration of VLANs on ports on a VLAN bridged network.
- **GVRP**: GARP VLAN Registration Protocol (GVRP) allows dynamic registration and de-registration of VLANs on ports on a VLAN bridged network.
- **Voice VLAN**: Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones.
- **MVR**: MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.
- **MSTP**: The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

- **VLAN ID**:

This field shows the identity of this particular VLAN.

- **VLAN Membership**:

These check boxes show membership for each VLAN ID.

7.11.4 Port Status

The **Port Status** sub-menu shows the port status classified by VLAN user.

To show VLAN Port Status:

1. Click **Configuration > VLAN > Port Status**.
2. Use the VLAN user drop-down box to select the specific VLAN user of the configuration or choose **Combined** to see all VLANs from any VLAN user.

Parameter description

- **Port:**

This field shows the port number for this row.

- **PVID:**

This field shows the VLAN identifier for this port.

- **Port Type:**

This field shows the port type.

- **Ingress Filtering:**

This field shows whether ingress filtering is **Enabled** or **Disabled** on this port.

- **Frame Type:**

This field shows whether the port accepts all frames or only tagged frames.

- **Tx Tag:**

This field shows whether frames are tagged before they're sent.

- **UVID:**

This field shows the untagged VLAN ID. The port's UVID determines how the frame is treated on the egress side.

- **Conflicts:**

This shows whether or not this port is involved in a conflict. The following conflicts can occur.

- Functional Conflicts between features.
- Conflicts due to hardware limitations.
- Direct conflict between user modules.

7.11.5 Private VLANs

Use the **Private VLANs** sub-menu to configure a group of ports to communicate only with an uplink port and not among themselves.

Private VLANs are based on source port masks, not the frame contents so they're not connected to IEEE 802.1Q VLANs. This means that VLAN IDs and Private VLAN IDs can be the same. A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1. A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

Private VLANs Membership

Use the **Private VLAN Membership** sub-menu to configure which ports are part of a private VLAN.

To configure Private membership:

1. Click **Configuration > VLAN > Private VLAN Membership**.
2. Click **Add New Private VLAN**.
3. Configure the parameters.
4. Click **Save**.

Parameter description

- **PVLAN ID:**

Use this field to configure the identity of this private VLAN.

- **Port Members:**

Use these check boxes to configure membership for each VLAN ID. No ports are members by default.

Port Isolation

Use the Port Isolation sub-menu to configure ports so they can only communicate with the uplink ports.

To configure Port Isolation:

1. Click **Configuration > VLAN > Private VLANs > Port Isolation**.
2. Configure the parameters.
3. Click **Save**.

Parameter description

- **Port Number:**

Use these check boxes to configure which ports are isolated. Port isolation is disabled on all ports by default.

7.11.6 MAC-Based VLAN

Use the **MAC-Based VLAN** sub-menu to configure a VLAN based on the source MAC address of untagged frames rather than port.

The most common way of grouping VLAN members is by port, hence the name port-based VLAN. Typically, the device adds the same VLAN tag to untagged packets that are received through the same port. Later on, these packets can be forwarded in the same VLAN. A port-based VLAN is easy to configure and is best suited to networks where the locations of hosts are fixed. As mobile office and wireless network access gain more popularity, the ports that terminal devices use to access the networks are very often non-fixed. A device may access a network through Port A this time, but through Port B the next time. If Port A and Port B belong to different VLANs, the device will be assigned to a different VLAN the next time it accesses the network. As a result, it will not be able to use the resources in the old VLAN. On the other hand, if Port A and Port B belong to the same VLAN, after terminal devices access the network through Port B, they will have access to the same resources as those accessing the network through Port A do, which brings security issues. MAC-based VLANs solve these problems.

MAC-based VLANs add a VLAN tag to an untagged frame according to its source MAC address. MAC-based VLANs are mostly used in conjunction with security technologies such as 802.1X to provide secure, flexible network access for terminal devices.

Configuration

Use the **Configuration** sub-menu to setup MAC-based VLANs.

To configure MAC-based VLANs:

1. Click **Configuration > VLAN > MAC address-based VLAN > Configuration**.
2. Click **Add new entry**.
3. Configure the parameters.
4. Click **Save**.

Parameter description

- **MAC Address:**

Use this field to configure any unicast MAC address for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed.

- **VLAN ID:**

Use this field to configure the VLAN identity.

- **Port Members:**

Use these check boxes to configure membership for each VLAN ID. No ports are members by default.

Status

Use the **Status** sub-menu to show MAC-based VLAN entries configured by **Static** or **NAS** (Network Access Server), or **Combined** MAC-based VLAN users.

To show MAC-based VLAN status:

1. Click **Configuration > VLAN > MAC-based VLAN > Status**.
2. Use the MAC-based VLAN user drop-down box to select the specific MAC-based VLAN user of the configuration or choose **Combined** to see all VLANs from any VLAN user.

Parameter description

- **MAC Address:**

This field shows the MAC address for this entry.

- **VLAN ID:**

This field shows the VLAN identity for this entry.

- **Port Members:**

This field shows the port members for the entry.

7.11.7 Protocol-Based VLAN

Use the **Protocol-Based VLAN** sub-menu to configure a VLAN based on layer-2 protocol numbers of untagged frames rather than port.

Protocol to Group

Use the **Protocol to Group** sub-menu to group protocol-matching criteria together under a group name.

To configure Protocol to Group mappings:

1. Click **Configuration > VLAN > Protocol-based VLAN > Protocol to Group**.
2. Click **Add new entry**.
3. Configure the parameters.
4. Click **Save**.

Parameter description

- **Frame Type:**

Use this drop-down box to configure which protocol to match. Possible configurations are:

- **Ethernet:**
- **LLC:** The Logical Link Control (LLC) data communication protocol layer is the upper sub-layer of the Data Link Layer (which is itself layer 2, just above the Physical Layer) in the seven-layer OSI reference model. It provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, Decnet and Appletalk) to coexist within a multipoint network and to be transported over the same network media, and can also provide flow control and automatic repeat request (ARQ) error management mechanisms.
- **SNAP:** The Subnetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier spaces. It is used with IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11 and other IEEE 802 physical network layers, as well as with non-IEEE 802 physical network layers such as FDDI that use 802.2 LLC.

- **Value:**

Use these fields to configure the protocol numbers for one of the following Frame Types.

- **Ethernet:** This field is an EtherType from 0x0600 to 0xffff.

- **LLC:** These are single-byte DSAP and SSAP fields each between 0x00 and 0xff.
- **SNAP:** These are the OUI (Organizationally Unique Identifier) and PID (Protocol ID) fields. If the OUI is zero, the protocol ID is the EtherType (0x0600-0xffff) of the protocol running on top of SNAP. If the OUI is not zero, the protocol ID is any 16-bit value assigned by that organization to the protocol running on top of SNAP.
- **Group Name:**
Use this field to configure a 16-character alphanumeric group name. This name must be unique across groups.

Group to VLAN

Use the **Group to VLAN** sub-menu to configure how Protocol-based VLAN groups map to VLAN IDs.

To configure Group to VLAN mappings:

1. Click **Configuration > VLAN > Protocol-based VLAN > Group to VLAN**.
2. Click **Add new entry**.
3. Configure the parameters.
4. Click **Save**.

Parameter description

- **Group Name:**
Use this field to configure a 16-character alphanumeric group name. The combination of this name and VLAN ID must be unique across entries and the group name must already be in the **Protocol to Group Mapping Table**.
- **VLAN ID:**
Use this field to configure the VLAN ID to which Group Name will be mapped.
- **Port Members:**
Use these check boxes to configure membership for each VLAN ID. No ports are members by default.

7.12 GARP and MRP

Use the **GARP** and **MRP** sub-menus to configure mechanisms for distributing attributes such as VLAN IDs.

The Generic Attribute Registration Protocol (GARP) is a legacy protocol that provides a generic framework for devices in a bridged LAN to register and de-register attributes such as VLAN Identifiers with each other. In doing so, the attributes are propagated to devices in the bridged LAN, and these devices form a reachability tree that is a subset of an active topology. GARP defines the architecture, rules of operation, state machines and variables for the registration and de-registration of attribute values.

GARP participation in a switch or an end station consists of a GARP application component, and a GARP Information Declaration (GID) component associated with each port or the switch. The propagation of information between GARP participants for the same application in a bridge is carried out by the GARP Information Propagation (GIP) component. Protocol exchanges take place between GARP participants by means of LLC Type 1 services, using the group MAC address and PDU format defined for the GARP application concerned. This switch has one GARP application: the GARP VLAN Registration Protocol (GVRP).

Multiple Registration Protocol (MRP) is the replacement for GARP. MRP allows participants in a MRP application to register attributes with other participants in a bridged LAN. The definition of attribute types, their values, and the semantics associated with values when registered, are specific to each MRP application. This switch has one MRP application: the Multiple VLAN Registration Protocol.

7.12.1 Configuration

Use the **Configuration** sub-menu to establish GARP/MRP for all switch ports.

To configure GARP/MRP:

1. Click **Configuration > GARP or MRP > Configuration**.
2. Configure the parameters.
3. Click **Save**.

Parameter description

- **Port:**

This shows the port number of this row.

- **Timer Values:**

Use this field to configure the following timers:

- **Join Timer:** The default value for Join timer is 200ms.
- **Leave Timer:** The range of values for Leave Time is 600-1000ms. The default value for Leave Timer is 600ms.
- **Leave All Timer:** The default value for Leave All Timer is 10000ms

- **Application:**

Use this drop-down box to configure the GARP or MRP application to **GVRP** or **MVRP**.

- **Attribute Type:**

Use this drop-down box to configure the types of attributes distributed by GARP/MRP to **VLAN**.

- **GARP/MRP Applicant:**

Use this drop-down box to configure the Applicant state machine behavior for GARP/MRP on this port to:

- **normal-participant:** In this default mode the Applicant state machine will operate normally in GARP/MRP protocol exchanges.
- **non-participant:** In this mode the Applicant state machine will not participate in the protocol operation.

7.12.2 Statistics

Use the **Statistics** sub-menu to show port statistics for GARP/MRP.

To show GARP/MRP statistics:

1. Click **Configuration > GARP or MRP > Statistics**.

Parameter description

- **Port:**

This field shows the port number of this row.

- **Peer MAC:**

This field shows the MAC address of the neighbor switch from which a GARP/MRP frame has been received.

- **Failed Count:**

This field shows the number of packets that couldn't be sent.

7.13 GVRP and MVRP

Use the **GVRP** or **MVRP** sub-menu to configure the GARP or MRP VLAN registration applications.

The GARP VLAN Registration Protocol (GVRP) and the Multiple VLAN Registration Protocol (MVRP) define an GARP/MRP application that provides the VLAN registrations service. GVRP/MVRP maintains dynamic VLAN registration entries for each VLAN and propagates these to other bridges. This information allows GVRP/MVRP-aware devices to dynamically establish and update their knowledge of the set of VLANs that have members and the ports through which these members can be reached.

7.13.1 Configuration

Use the Configuration sub-menu to setup GVRP/MVRP for all switch ports.

To configure GVRP/MVRP:

1. Click **Configuration > GVRP or MVRP > Configuration**.
2. Configure the Parameters.
3. Click **Save**.

Parameter description

Global Configuration

- **GVRP/MVRP Mode:**

Use this drop-down box to **Enable** or **Disable** (default) GVRP/MVRP mode on this port.

Port Configuration

- **Port:**

This field shows the port number of this row.

- **GVRP/MVRP Mode:**

Use this drop-down box to **Enable** or **Disable** (default) GVRP/MVRP mode on this port.

- **GVRP/MVRP rrole:**

Use this drop-down box to configure the restricted role to **Enable** or **Disable** on this port.

7.13.2 Statistics

Use the **Statistics** sub-menu to show port statistics for GVRP/MVRP.

To show GVRP/MVRP statistics, click **Configuration > GVRP or MVRP > Statistics**.

Parameter description

- **Port:**

This field shows the port number of this row.

- **Join Tx Count:**

This field shows the number of join events sent from this port.

- **Leave Tx Count:**

This field shows the number of leave events sent from this port.

7.14 QoS

The switch support four QoS queues per port with strict or weighted fair queuing scheduling. It supports QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP and UDP/TCP ports and ranges. High flexibility in the classification of incoming frames to a QoS class. The QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS class assigned to a frame is used throughout the device for providing queuing, scheduling, and congestion control guarantees to the frame according to what was configured for that specific QoS class. The switch support advanced memory control mechanisms providing excellent performance of all QoS classes under any traffic scenario, including jumbo frame. A super priority queue with dedicated memory and strict highest priority in the arbitration. The ingress super priority queue allows traffic recognized as CPU traffic to be received and queued for transmission to the CPU even when all the QoS class queues are congested.

7.14.1 Port Classification

Use the **Port Classification** sub-menu to configure basic QoS ingress classification for all switch ports.

To configure the QoS port classification parameters:

1. Click **Configuration > QoS > Port Classification**.
2. Configure the parameters.
3. Click **Save**.
4. Click a **Tag Class** to configure ingress tag classification for this port.
5. Configure the parameters.
6. Click **Save**.

Parameter description

Port Classification page

- **Port:**

This shows the logical port number of this row.

- **QoS class:**

Use this drop-down box to configure the default QoS class for frames not classified in any other way. There is a one to one mapping between QoS class, queue and priority. A QoS class of zero has the lowest priority.

- **DP level:**

Use this drop-down box to configure the default Drop Precedence Level for frames not classified in any other way.

- **PCP:**

Use this drop-down box to configure the default Priority Code Point for untagged frames.

- **DEI:**

Use this drop-down box to configure the default Drop Eligibility Indicator for untagged frames.

- **Tag Class:**

This shows the following classification modes for tagged frames on this port.

- **Disabled:** Use default QoS class and DP level for tagged frames.

- **Enabled:** Use mapped versions of PCP and DEI for tagged frames. **(PCP,DEI) to (QoS class, DP level) Mapping** on the **QoS Ingress Port Tag Classification** page for this port controls the mapping of classified (PCP, DEI) to (QoS class, DP level) values.

Click the mode to configure the mode and/or mapping on the **QoS Ingress Port Tag Classification** page.

- **DSCP Based:**

Use this check box to enable DSCP-based QoS ingress port classification.

QoS Ingress Port Tag Classification page

- **Tag Classification:**

Use this drop-down box to **Enable** or **Disable** tag classification.

- **PCP:**

This field shows the default Priority Code Point for untagged frames.

- **DEI:**

This field shows the default Drop Eligibility Indicator for untagged frames.

- **QoS class:**

Use this drop-down box to configure the default QoS class for frames not classified in any other way. There is a one to one mapping between QoS class, queue and priority. A QoS class of zero has the lowest priority.

- **DP level:**

Use this drop-down box to configure the default Drop Precedence Level for frames not classified in any other way.

7.14.2 Port Policing

Use the **Port Policing** sub-menu to constrain traffic flows and mark frames that are part of flows above set rates. Policing is primarily useful for voice or video flows because they usually maintain a steady rate of traffic.

To configure QoS Port Policing:

1. Click **Configuration > QoS > Port Policing**.
2. Click the port number to configure the policer for that port.
3. Configure the parameters.
4. Click **Save**.

Parameter description

- **Policer:**

This column header shows the policer number of **1** to **4**.

- **Enabled:**

Check these check boxes to enable policers for this port.

- **Rate and Rate Unit:**

Use these fields and drop-down boxes to limit the data rate (default is 500) for this port.

- **DP Bypass Level:**

Use these drop-down boxes to configure the drop precedence bypass level. Frames with a Drop Precedence Level below the bypass level are not policed.

- **Unicast, Multicast and Broadcast:**

Check these check boxes to enable unicast, multicast and broadcast frames to be policed.

- **Flooding:**

Check these check boxes to configure flooded frames to be policed.

- **Learning:**

Check these check boxes to police the rate at which the switch can add entries to its CAM.

- **Flow Control:**

Check these check boxes to send pause frames instead of dropping frames when the policed data rate is reached. Pause frames are only sent if the port is in flow control mode.

7.14.3 Queue Policing

Use the **Queue Policing** sub-menu to constrain traffic flows into each queue. Queue policing is primarily useful for voice or video flows because they usually maintain a steady rate of traffic.

To configure QoS Queue Policing:

1. Click **Configuration > QoS > Queue Policing**.
2. Configure the parameters.
3. Click **Save**.

Parameter description

- **Port:**

This shows the port number of this row.

- **Enabled:**

Check these check boxes to enable queue policers on this port.

- **Rate and Unit:**

Use these fields and drop-down boxes to limit the data rate (default is 500) for this queue. This value is restricted to 100 to 1000000 kbps or 1 to 13200 Mbps.

7.14.4 Port Scheduler and Port Shaping

Use the **Port Scheduler** and **Port Shaping** sub-menus to configure QoS egress port schedulers and shapers for all switch ports.

To configure QoS port scheduling and shaping:

1. Click **Configuration > QoS > Port Scheduler** or **Port Shaping**.
2. Click the port number to configure the schedulers. The **QoS Egress Port Schedulers and Shapers** page appears.
3. Configure the parameters.
4. Click **Save**.

Parameter description

- **Scheduler Mode:**

Use this drop-down box to configure the scheduler mode to **Strict Priority** or **Weighted** for this port.

Queue Shaper

- **Enable:**

Check these check boxes to enable queue shapers on this port.

- **Rate and Unit:**

Use these fields and drop-down boxes to limit the data rate (default is 500) for this queue. This value is restricted to 100 to 1000000 kbps or 1 to 13200 Mbps.

- **Excess:**

Check this check box to allow the queue to use excess bandwidth.

Queue Scheduler

These parameters appear when **Scheduler Mode** is **Weighted**.

- **Weight:**

Use this field to configure the weight (default is 17) for this queue. This value is restricted to 1 to 100.

- **Percent:**

This field shows the weight in percent for this queue.

Port Shaper

- **Enable:**

Check this check box to enable port shaper on this port.

- **Rate and Unit:**

Use these fields and drop-down boxes to limit the data rate (default is 500) for this queue. This value is restricted to 100 to 1000000 kbps or 1 to 13200 Mbps.

7.14.5 Port Tag Remarking

Use the **Port Tag Remarking** sub-menu to configure how the PCP and DEI fields are re-marked at the egress of switch ports.

To configure QoS port tag re-marking:

1. Click **Configuration > QoS > Port Tag Remarking**.
2. Click the port number to configure the tag re-marking. The **QoS Egress Port Tag Remarking** page appears.
3. Configure the parameters.
4. Click **Save**.

Parameter description

- **Tag Remarking Mode:**

Use this drop-down box to configure how egress frames are re-marked. Possible values are:

- **Classified:** Use classified PCP/DEI values.
- **Default:** Use default PCP/DEI values.
- **Mapped:** Use mapped versions of QoS class and DP level.

PCP/DEI Configuration

These parameters appear when **Tag Remarking Mode** is **Default**.

- **Default PCP:**

Use this drop-down box to configure the default Priority Code Point.

- **Default DEI:**

Use this drop-down box to configure the default Drop Eligibility Indicator.

DP level Configuration

These parameters appear when **Tag Remarking Mode** is **Mapped**.

- **Classified DP Level:**

This field shows the two-bit classified DP level for this row.

- **DP Level:**

Use this drop-down box to configure the single-bit DP Level used in the (QoS class, DP level) to (PCP, DEI) mapping.

(QoS class, DP level) to (PCP, DEI) Mapping

These parameters appear when **Tag Remarking Mode** is **Mapped**.

- **QoS class:**

This field shows the QoS class for this row. There is a one to one mapping between QoS class, queue and priority. A QoS class of zero has the lowest priority.

- **DP level:**

This field shows the Drop Precedence Level for this row.

- **PCP:**

Use this drop-down box to configure the Priority Code Point written to egress frames.

- **DEI:**

Use this drop-down box to configure the Drop Eligibility Indicator written to egress frames.

7.14.6 Port DSCP

Use the **Port DSCP** sub-menu to configure on a port-by-port basis how the DSCP field is changed on ingress and egress packets.

To configure Port DSCP:

1. Click **Configuration > QoS > Port DSCP**.
2. Configure the parameters
3. Click **Save**.

Parameter description

- **Port:**

This shows the port number for this row.

- **Ingress Translate:**

Check this check box to enable incoming translation (change the DSCP field on ingress packets).

- **Ingress Classify:**

Use this drop-down box to configure how incoming packets are classified into flows.

- **Disable:** Don't classify any packets.
- **DSCP=0:** Classify packets that have a DSCP of 0.
- **Selected:** Classify packets with one of a set of selected DSCPs. These selected DSCPs are those whose **Ingress Classify** check box is checked in the **DSCP Translation** page.
- **All:** Classify all packets.

- **Egress:**

Use this drop-down box to configure how packets leaving the switch have their DSCP fields changed.

- **Disable:** Don't rewrite any packets.
- **Enable:** Rewrite the DSCP field without re-mapping it.
- **Remap:** Rewrite the DSCP with the re-mapped DSCP.

7.14.7 DSCP Based QoS

Use the **DSCP-Based QoS** sub-menu to configure how the DSCPs on incoming packets are mapped to internal QoS Class and DPL values.

To configure DSCP-based QoS:

1. Click **Configuration > QoS > DSCP-Based QoS**.
2. Configure the parameters.
3. Click **Save**.

Parameter description

- **DSCP:**

This field shows the DSCP for this row.

- **Trust:**

Check this check box to trust this DSCP value.

- **QoS Class:**

Use this drop-down box to configure the QoS class for this row.

- **DPL:**

Use this drop-down box to configure the Drop Precedence Level for this row.

7.14.8 DSCP Translation

Use the **DSCP Translation** sub-menu to configure how DSCPs are translated on ingress packets and remapped on egress packets.

To configure DSCP Translation:

1. Click **Configuration > QoS > DSCP Translation**.
2. Configure the parameters.
3. Click **Save**.

Parameter description

- **DSCP:**

This field shows the DSCP for this row.

- **Ingress Translate:**

Use this drop-down box to configure the translated DSCP that is used for QoS class and DPL mapping of incoming packets.

- **Ingress Classify:**

Check this check box to specify this DSCP be used to classify incoming packets

- **Egress Remap:**

Use this drop-down box to configure which DSCP is used on egress packets.

7.14.9 DSCP Classification

Use the **DSCP Classification** sub-menu to map DSCPs to QoS Classes.

To configure DSCP Classification:

1. Click **Configuration > QoS > DSCP Classification**.
2. Configure the Parameters.
3. Click **Save**.

Parameter description

- **QoS Class:**

This field shows the QoS Class for this row.

- **DSCP:**

Use this drop-down box to configure a DSCP for this row.

7.14.10 QoS Control List

Use the **QoS Control List** sub-menu to configure up to 256 QoS Control Entries for finer grained control over QoS class, DPL and DSCP.

To configure the QoS Control List:

1. Click **Configuration > QoS > QoS Control List**.
2. Click one of the following icons to view, add or edit an QCE:

 : Inserts a new QCE before the current row.

 : Edits the QCE row.

 : Moves the QCE up the list.

 : Moves the QCE down the list.

 : Deletes the QCE.

 : The lowest plus sign adds a new entry at the bottom of the QCE listings.

3. Configure the parameters.
4. Click **Save**.

Parameter description

QCE parameters consist of conditions that must match to trigger a QCE and the actions that are carried out when an QCE is triggered.

QCE Conditions

The items shown on the **QCE Configuration** page depend on the conditions selected. E.g. select a **Frame Type** of **Ethernet Type** and the **Ethernet Type Parameters** item appears. The items that don't change are as follows.

- **Port Members:**

Use these check boxes to configure which ports can contribute traffic to be inspected by this QCE. All ports are enabled by default.

- **Tag:**

Use this drop-down box to configure whether **Any**, **Untagged** or **Tagged** frames match this QCE.

- **VID:**

Use this drop-down box and these fields to configure this QCE to match **Any** VLAN ID a **Specific** VLAN ID or a **Range** of VLAN IDs.

- **PCP:**

Use this drop-down box to configure which Priority Code Points match this QCE.

- **DEI:**

Use this drop-down box to configure which Drop Eligible Indicators match this QCE.

- **SMAC:**

Use this drop-down box to configure which most significant 24 bits of the source MAC address matches this QCE.

- **DMAC Type:**

Use this drop-down box to configure which destination MAC address match this QCE. Possible values are:

- **Any:** The QCE matches any address.
- **MC:** The QCE matches multicast addresses.
- **BC:** The QCE matches broadcast addresses.
- **UC:** The QCE matches any unicast address.

- **Frame Type:**

Use this drop-down box to configure which frame type matches this QCE. Possible frame types are:

- **Any:** The QCE matches any frame type.
- **Ethernet Type:** The QCE matches Ethernet frames with EtherTypes of 0x0600 to 0xFFFF. **Ethernet Type Parameters** appears when this is chosen.
- **LLC:** The QCE matches LLC frames.
- **SNAP:** The QCE matches SNAP frames.
- **IPv4:** The QCE matches any IPv4 packets.
- **IPv6:** The QCE matches any IPv6 packets.

Ethernet Type Parameters

- **EtherType Filter:**

Use this drop-down box to configure which Ethernet Length/Type field values match this QCE. Choose **Any** to configure this QCE to match frames with an Ethernet Length/Type field of 0x0600 to 0xFFFF excluding 0x0800 (IPv4) and 0x86DD (IPv6). Choose **Specific** and then complete the **Ethernet Type Value** field to match a specific Ethernet Length/Type. Ethernet Type Values less than 0x0600 or equal to 0x0800 (IPv4) or 0x86DD (IPv6) cannot be configured.

LLC Parameters

- **SSAP Address:**

Use this drop-down box to configure which Source Service Access Point (SSAP) address matches this QCE. Choose **Any** to configure this QCE to ignore the SSAP. Choose **Specific** and then complete the **Value** field to match a specific SSAP from 0 to 0xFF.

- **DSAP Address:**

Use this drop-down box to configure which Destination Service Access Point (DSAP) address matches this QCE. Choose **Any** to configure this QCE to ignore the DSAP. Choose **Specific** and then complete the **Value** field to match a specific DSAP from 0 to 0xFF.

- **Control:**

Use this drop-down box to configure which control address matches this QCE. Choose **Any** to configure this QCE to ignore the control address. Choose **Specific** and then complete the **Value** field to match a specific control address from 0 to 0xFF.

SNAP Parameters

- **PID:**

Use this drop-down box to configure which Protocol ID matches this QCE. Choose **Any** to configure this QCE to ignore the PID. Choose **Specific** and then complete the **Value** field to match a specific PID from 0 to 0xFFFF.

IPv4 Parameters

- **Protocol:**

Use this drop-down box to configure which protocol in the IP header matches this QCE. Choose **Any** to configure this QCE to ignore the protocol. Choose **UDP** or **TCP** or choose **Other** and then complete the **IP Protocol Value** field match another protocol.

- **Source IP:**

Use this drop-down box to configure which source IP address field values matches this QCE. Choose **Any** to configure this QCE to ignore the source IP address field. Choose **Specific** and then complete the **Value** and **Mask** fields to match all source IP addresses within a network.

- **IP Fragment:**

Use this drop-down box to configure this QCE to match the IPv4 fragmented flag.

- **DSCP:**

Use this drop-down box to configure this QCE to match the DSCP.

UDP and TCP Parameters

- **SPort and DPort**

Use these drop-down boxes to configure which TCP/UDP source port and TCP/UDP destination port field values match this QCE. Choose **Any** to configure this QCE to ignore the source/destination port field. Choose **Specific** and then complete the **Value** field to match a specific source or destination port. Choose **Range** and then complete the **From** and **To** fields to match a range of source or destination ports.

IPv6 Parameters

- **Protocol:**

Use this drop-down box to configure which protocol in the IP header matches this QCE. Choose **Any** to configure this QCE to ignore the protocol. Choose **UDP** or **TCP** or choose **Other** and then complete the **IP Protocol Value** field match another protocol.

- **Source IP (32 LSB):**

Use this drop-down box to configure which least significant 32-bits of source IP address field values matches this QCE. Choose **Any** to configure this QCE to ignore the source IP address field. Choose **Specific** and then complete the **Value** and **Mask** fields to match all source IP addresses within a network.

- **DSCP:**

Use this drop-down box to configure this QCE to match the DSCP.

QCE Actions

- **Class:**

Use this drop-down box to configure which queue frames are put in if this QCE is triggered.

- **DPL:**

Use this drop-down box to configure which drop precedence level is set if this QCE is triggered.

- **DSCP:**

Use this drop-down box to configure which DSCP is set if this QCE is triggered.

7.14.11 QCL Status

Use the **QCL Status** sub-menu to get an overview of the status of all QCEs used across the device.

To show the QoS Control List Status

1. Click **Configuration > QoS > QCL Status**.
2. Select the part of the device that uses this QCL from the QCL User drop-down box.

Parameter description

- **User:**

This field shows the QCE user.

- **QCE#:**

This field shows the QCE number.

- **Frame Type:**

This field shows which Ethernet frame type matches this QCE. Possible values are:

- **Any:** The QCE matches any frame type.
- **Ethernet Type:** The QCE matches Ethernet frames with EtherTypes of 0x0600 to 0xFFFF.
- **LLC:** The QCE matches LLC frames.
- **SNAP:** The QCE matches SNAP frames.
- **IPv4:** The QCE matches any IPv4 packets.
- **IPv6:** The QCE matches any IPv6 packets.

- **Port:**

This field shows the list of ports that match this QCE.

- **Action:**

This group of fields shows the classification action taken on ingress frames if the QCE is triggered.

- **Class:** This shows which queue frames are put in if this QCE is triggered.
- **DP:** This shows which drop precedence level is set if this QCE is triggered.

- **DSCP:** This shows which DSCP is set if this QCE is triggered.
- **Conflict:**
This field shows whether the QCE has not been applied to the hardware due to hardware limitations.
- **Resolve Conflict:**
Click this button to resolve a conflict.

7.14.12 WRED

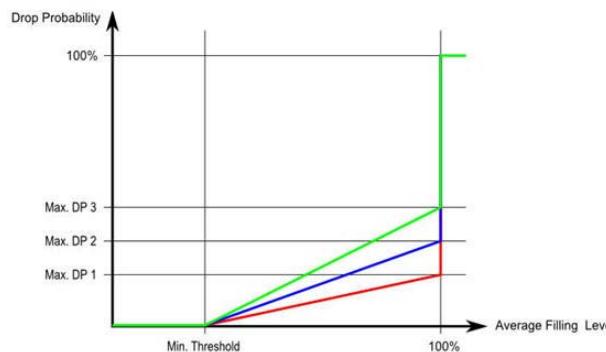
Use the WRED sub-menu to configure Weighted Random Early Detection.

Classic Random Early Detection (RED) monitors the average queue size and drops or marks packets based on statistical probabilities. If the buffer is almost empty all incoming packets are accepted. As the queue grows, the probability for dropping an incoming packet grows too. When the buffer is full the probability has reached 1 and all incoming packets are dropped.

RED is more fair than tail drop, in the sense that it does not possess a bias against burst traffic that uses only a small portion of the bandwidth. The more a host transmits, the more likely it is that its packets are dropped as the probability of a host's packet being dropped is proportional to the amount of data it has in a queue. Early detection helps avoid TCP global synchronization.

There were two bugs in classic RED, so improvements to the algorithm were developed. A draft paper was prepared but never published, so the improvements were not widely implemented. Pure RED does not accommodate quality of service (QoS) differentiation. WRED and RED with In and Out (RIO) provide early detection with QoS considerations.

The following illustration shows the drop probability function with associated parameters.



Max. DP 1-3 is the drop probability when the average queue filling level is 100%. Frames marked with Drop Precedence Level 0 are never dropped. Min. Threshold is the average queue filling level where the queues randomly start dropping frames. The drop probability for frames marked with Drop Precedence Level n increases linearly from zero (at Min. Threshold average queue filling level) to Max. DP n (at 100% average queue filling level).

To configure WRED:

1. Click **Configuration > QoS > WRED**.
2. Configure the parameters.
3. Click **Save**.

Parameter description

- **Queue:**

This field shows the queue number (QoS class) for this row.

- **Enable:**

Use this check box to configure whether RED is enabled for this queue.

- **Min. Threshold:**

Use this field to configure the lower RED threshold. If the average queue filling level is below this threshold, the drop probability is zero. This value is restricted to between 0 and 100.

- **Max. DP1, Max. DP2 and Max. DP3:**

Use this field to configure the drop probability for frames marked with Drop Precedence Level 1, 2 or 3 when the average queue filling level is 100%. This value is restricted to between 0 and 100.

7.15 sFlow Agent

Use the **sFlow Agent** sub-menu to configure the switch to sample traffic and send statistics or partial packet captures to a centrally located sFlow Collector for analysis.

7.15.1 Collector

Use the **Collector** sub-menu to configure where the sFlow samples are sent.

To configure sFlow collector attributes:

1. Click **Configuration > sFlow Agent > Collector**.
2. Configure the Parameters.
3. Click **Save**.

Parameter description

- **Receiver Id:**

This field shows the identity of this particular sFlow receiver.

- **IP Type:**

Use this drop-down box to configure whether the collector supports **IPv4** or **IPv6**.

- **IP Address:**

Use this field to configure which IP address sFlow samples are sent.

- **Port:**

Use this field to configure which UDP port (default **6343**) sFlow samples are sent.

- **Time out:**

Use this field to configure how long the sFlow agent in the switch sends samples.

- **Datagram Size:**

Use this field to configure the maximum UDP datagram size (default **1400** bytes) used for sending samples. This must be from **200** to **1500** bytes.

7.15.2 Sampler

Use the **Sampler** sub-menu to configure how the sFlow agent samples traffic on a port-by-port basis.

To configure the sampler:

1. Click **Configuration > sFlow Agent > sampler**.
2. Click  on the port number to edit the sFlow sampler parameters.
3. Configure the parameters.
4. Click **Save**.

Parameter description

- **sFlow Port:**

This field shows the port that is being configured.

- **sFlow Instance:**

This field shows the sFlow instance for this port.

- **Sampler Type:**

Use this drop-down box to configure what is sampled on this port. Choose **None** (default) to disable sampling, **RX** to sample traffic received, **TX** to sample traffic sent or **ALL** to sample both sent and received traffic.

- **Sampling Rate:**

Use this field to configure the switch to sample one in this number of frames. This can be from **0** (disabled) to **4095**.

- **Max Hdr Size:**

Use this field to configure the amount of the frame header (default 128 bytes) that is sampled. This must be from **14** to **200** bytes.

- **Polling Interval:**

Use this field to configure how often counters are sampled. This can be from **0** (disabled) to **3600** seconds.

7.16 Mirroring

Use the **Mirroring** sub-menu to configure how traffic from one or more ports is copied to another (mirror) port. This enables real-time traffic analysis of traffic crossing the source port in a completely unobtrusive manner.

To configure mirroring:

1. Click **Configuration > Mirroring**.
2. Configure the parameters.
3. Click **Save**.

Parameter description

- **Port to mirror on:**

Use this drop-down box to configure the port where traffic is mirrored to.

- **Port:**

This field shows the logical port for this row.

- **Mode:**

Use this drop-down box to configure which traffic is mirrored. Choose **Rx only** to mirror frames received on this port. Choose **Tx only** to mirror frames transmitted on this port. Choose **Enabled** to mirror frames received and transmitted on this port.

Note:

For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames on the mirror port. Because of this, the mode for the selected mirror port is limited to **Disabled** or **Rx only**.

7.17 Trap Event Severity

Use the **Trap Event Severity** sub-menu to configure which events will be sent to the system log.

To configure Trap Event Severity:

1. Click **Configuration > Trap Event Severity Configuration**.
2. Configure the parameters.
3. Click **Save**.

Parameter description

- **Group Name:**

The field shows the type of events that can be logged.

- **Severity Level:**

Use this drop-down box to configure the event severity required to cause events to be logged.

7.18 SMTP Configuration

Use the SMTP Configuration sub-menu to send events to an SMTP server.

To enable events to be sent to an SMTP server:

1. Click **Configuration > SMTP Configuration**.
2. Configure the parameters.
3. Click **Save**.

Parameter description

- **Mail Server:**

Use this field to configure the IP Address of the SMTP server.

- **User Name and Password:**

Use this field to configure the user name and password that the switch logs into the SMTP server with.

- **Severity Level:**

Use this drop-down box to configure the event severity required to cause events to be logged.

- **Sender:**

Use this field to configure the SMTP sender name.

- **Return-Path:**

Use this field to configure the SMTP return email address.

- **Email Address 1-6:**

Use these fields to configure the destination email addresses to send events to.

7.19 802.3ah OAM

Use the **802.3ah OAM** sub-menu to configure Link Layer Operations Administration and Maintenance.

Carrier ethernet applications that customer need to reduce operating cost and increase the remote maintain availability. The advent of Ethernet as a metropolitan and wide-area networking technology has accelerated the need for a new set of OAM protocols. Service provider networks are large and complex with a wide user base, and they often involve different operators that must work together to provide end-to-end services to enterprise customers. While enterprise end-customer demands continue to increase, so do the requirements for service provider Ethernet networks, particularly in the areas of availability and mean time to repair (MTTR). Ethernet OAM addresses these challenges and more, thereby directly impacting the competitiveness of the service provider. Ethernet has been used as a LAN technology for many years, and enterprises have managed these networks effectively, Ethernet OAM is a broad topic, but this paper will focus on three main areas of Ethernet OAM that are most in need by service providers and are rapidly evolving in the standards bodies: Service Layer OAM (IEEE 802.1ag Connectivity Fault Management), Link Layer OAM (IEEE 802.3ah OAM), and Ethernet Local Management Interface (MEF-16 E-LMI). Each of these different OAM protocols has unique objectives and is complementary to the others. IEEE 802.1ag Connectivity Fault Management provides service management.

7.19.1 Port Config

Use the **Port Config** sub-menu to configure Link OAM port parameters.

To configure 802.3ah OAM on a port-by-port basis:

1. Click **Configuration > 802.3ah OAM > Port config**.
2. Click a port number to see the **Detailed Link OAM Status** page or configure the parameters and click **Save**.

Parameter description

- **Port:**

This field shows the port number for this row.

- **OAM Enabled:**

Check this check box to enable OAM on this port.

- **OAM Mode:**

Use this drop-down box to configure this port to initiate the discovery process (**Active** mode) or not to initiate the discovery process (default **Passive** mode). After the discovery process active ports can send any OAMPDU while connected to a remote OAM peer. Active ports don't respond to OAM remote loopback commands and variable requests from a passive peer. Passive ports react to the initiation of the discovery process to prevent passive to passive links. Passive ports don't send Variable Request or Loopback Control OAMPDUs.

- **Loopback support:**

Check this check box to enable this port to execute the remote loopback command that helps fault localization and link performance testing.

- **Link Monitor support:**

Use this check box to configure whether this port supports event notification that permits the inclusion of diagnostic information.

- **MIB Retrieval Support:**

Use this check box to configure whether this port supports polling of various Link OAM based MIB variables.

- **Loopback Operation:**

Check this check box to start a loopback operation on this port.

7.19.2 Event Config

Use the **Event Config** sub-menu to configure which events trigger the 802.3ah OAM monitoring and management function.

To configure link events:

1. Click **Configuration > 802.3ah OAM > Event Config**.
2. Choose a port number from the port drop-down box next to the **Auto-refresh** check box.
3. Configure the parameters.
4. Click **Save**.

Parameter description

- **Event Name:**

This column shows the name of the link event that will be monitored by the switch.

- **Error Frame Event:**

The Error Frame Event counts the number of error frames detected during the time defined by the **Window (100 msec)** field and generates an event if the error frame count is equal to or greater than the threshold (**Period Threshold**) for that time window. Error frames are frames that had transmission errors as detected at the Media Access Control sub-layer.

- **Event Seconds Summary:**

The Error Frame Seconds Summary Event counts the number of error frame seconds that occurred during the time defined by the **Window (100 msec)** field and generates an event if the error frame count is equal to or greater than the threshold (**Period Threshold**) for that time window. An error frame second is a one second interval wherein at least one frame error was detected. Error frames are frames that had transmission errors as detected at the Media Access Control sub layer.

- **Symbol Period Error Event:**

The Error Symbol Period Event counts the number of symbol errors that occurred during the time defined by the **Window (100 msec)** field and generates an event if the error symbol count is equal to or greater than the threshold (**Period Threshold**) for that time window. The time period is specified in the **Window (100 msec)** field as the number of symbols that can be received in this time period on the underlying physical layer.

- **Frame Period Error Event:**

The Error Frame Period Event counts the number of error frames that occurred during the time defined by the **Window (100 msec)** field and generates an event if the error frame count is equal to or greater than the threshold (**Period Threshold**) for that time window. The period is specified in the **Window (100 msec)** field as the number of frames that can be received in this time period. Error frames are frames that had transmission errors as detected at the Media Access Control sub layer.

- **Window (100 msec):**

Use this field to configure the window for the observation of link events.

- **Period Threshold:**

Use this field to configure the threshold that must be reached during the window period for a link event to be generated.

- **RxPacket Threshold:**

Use this field to configure the number of events that must be collected during the window period before the peer is notified.

7.19.3 Port Status

Use the Port Status sub-menu to show the local and remote state of 802.3ah OAM on a port-by-port basis.

To show the 802.3ah OAM port status:

1. Click **Configuration > 802.3ah OAM > Port Status**.
2. Choose a port number from the port drop-down box next to the **Auto-refresh** check box.

Parameter description

- **PDU Permission:**

This field shows the current permission rule-set for the local port. Possible values are **Link fault, Receive only, Information exchange only or ANY**.

- **Discovery State:**

The field shows the current state of the discovery process. The possible states are **Fault state, Active state, Passive state, SEND_LOCAL_REMOTE_STATE, SEND_LOCAL_REMOTE_OK_STATE, SEND_ANY_STATE**.

- **Remote MAC Address:**

This field shows the MAC address of the remote device.

- **Mode:**

The field shows the OAM Mode that the port is operating in (**Active or Passive**).

- **Unidirectional Operation Support:**

The field shows the whether the PHY supports unidirectional operation.

- **Remote Loopback Support:**

This field shows whether the port is capable of OAM remote loopback mode.

- **Link Monitoring Support:**

This field shows whether the port can interpret link events.

- **MIB Retrieval Support:**

This field shows whether the ports can send Variable Response OAMPDUs.

- **MTU Size:**

This field shows the largest OAMPDU in octets supported by this port. This value is compared to the remote port's Maximum PDU Size and the smaller of the two is used.

- **Multiplexer State:**

This field shows whether the OAM multiplexer on this port is forwarding non-OAMPDUs to the lower sub-layer or discarding them.

- **Parser State:**

This field shows whether the OAM parser on this port is forwarding non-OAMPDUs to the higher sub-layer or looping them back through the lower sub-layer. When in the discarding state this port discards non-OAMPDUs.

- **Organizational Unique Identification:**

This field shows the 24-bit Organizationally Unique Identifier of the vendor.

- **PDU Revision:**

This field shows the current revision of the Information TLV. This value starts at zero and is incremented each time something in the Information TLV changes. Upon reception of an Information TLV from a peer, an OAM client may use this field to decide if it needs to be processed. An Information TLV that is identical to the previous Information TLV doesn't need to be parsed as nothing in it has changed.

7.19.4 Link Events

Use the **Link Events** sub-menu to show 802.3ah OAM link event statistics.

To show link event statistics:

1. Click **Configuration > 802.3ah OAM > Link Events**.
2. Choose a port number from the port drop-down box next to the **Auto-refresh** check box.

Parameter description

Local and Remote Frame Error Status

- **Frame Error Event Timestamp:**

This two-octet field shows when the event was generated in 100-millisecond units.

- **Frame Error Event Window:**

This two-octet field shows the duration of the window for the observation of Error Frame Events in 100-millisecond units.

- **Frame Error Event threshold:**

This four-octet field shows the number of error frames that must be detected during the window period for a link event to be generated.

- **Frame Errors:**

This four-octet field shows the number of detected error frames in the window period.

- **Total Frame Errors:**

This eight-octet field shows the number of error frames that have been detected since the OAM sub-layer was reset.

- **Total Frame Error Events:**

This four-octet field shows the number of Error Frame Event TLVs that have been generated since the OAM sub-layer was reset.

Local and Remote Frame Period Status

- **Frame Period Error Event Timestamp:**

This two-octet field shows when the event was generated in 100-millisecond units.

- **Frame Period Error Event Window:**

This four-octet field shows the duration of the window for the observation of Error Frame Events in terms of frames.

- **Frame Period Error Event Threshold:**

This four-octet field shows the number of error frames that must be detected during the window period for a link event to be generated.

- **Frame Period Errors:**

This four-octet field shows the number of detected error frames in the window period.

- **Total Frame Period Errors:**

This eight-octet field shows the number of error frames that have been detected since the OAM sub-layer was reset.

- **Total Frame Period Error Events:**

This four-octet field shows the number of Error Frame Event TLVs that have been generated since the OAM sub-layer was reset.

Local and Remote Symbol Period Status

- **Symbol Period Error Event Timestamp:**

This two-octet field shows when the event was generated in 100-millisecond units.

- **Symbol Period Error Event Window:**

This eight-octet field shows the duration of the window for the observation of error symbols in terms of symbols.

- **Symbol Period Error Event Threshold:**

This eight-octet field shows the number of error symbols that must be detected during the window period for a link event to be generated.

- **Symbol Period Errors:**

This eight-octet field shows the number of detected error symbols in the window period.

- **Symbol Frame Period Errors:**

This eight-octet field shows the number of error symbols that have been detected since the OAM sub-layer was reset.

- **Symbol Frame Period Error Events:**

This four-octet field shows the number of Error Symbol Period Event TLVs that have been generated since the OAM sub-layer was reset.

Local and Remote Event Seconds Summary Status

- **Event Seconds Summary Timestamp:**

This two-octet field shows when the event was generated in 100-millisecond units.

- **Event Seconds Summary Window:**

This two-octet field shows the duration of the window for the observation of error frame seconds in 100-millisecond units. An error frame second is a one second interval wherein at least one frame error was detected.

- **Event Seconds Summary Threshold:**

This two-octet field shows the number of error frame seconds that must be detected during the window period for a link event to be generated. An error frame second is a one second interval wherein at least one frame error was detected.

- **Event Seconds Summary Events:**

The field shows this two-octet field indicates the number of error frames in the period.

- **Event Seconds Summary Error Total:**

This four-octet field shows the number of error frame seconds that have been detected since the OAM sub-layer was reset.

- **Event Seconds Summary Event Total:**

This four-octet field shows the number of Errored Frame Seconds Summary Event TLVs that have been generated since the OAM sub-layer was reset.

7.19.5 Statistics

Use the **Statistics** sub-menu to show OAMPDU statistics on a port-by-port basis.

To show the OAMPDU statistics:

1. Click **Configuration > 802.3ah OAM > Statistics**.
2. Choose a port number from the port drop-down box next to the **Auto-refresh** check box.

Parameter description

- **Rx and Tx OAM Information PDUs:**

This field shows the number of received and transmitted OAM Information PDUs. Discontinuities of this counter can occur at re-initialization of the management system.

- **Rx and Tx Unique Error Event Notification:**

This field shows the number of Event OAMPDUs received and transmitted with unique OAMPDU Sequence Numbers on this interface. Event Notification OAMPDUs may be resent to reduce the chance of loss. This field doesn't count duplicates.

- **Rx and Tx Duplicate Error Event Notification:**

This field shows the number of Event OAMPDUs received and transmitted with duplicate OAMPDU Sequence Numbers on this interface. Event Notification OAMPDUs may be resent to reduce the chance of loss. This field counts the original as well as the duplicates.

- **Rx and Tx Loopback Control:**

This field shows the number of Loopback Control OAMPDUs received and transmitted on this interface.

- **Rx and Tx Variable Request:**

This field shows the number of Variable Request OAMPDUs received and transmitted on this interface.

- **Rx and Tx Variable Response:**

This field shows the number of Variable Response OAMPDUs received and transmitted on this interface.

- **Rx and Tx Org Specific PDU's:**

This field shows the number of Organization Specific OAMPDUs transmitted on this interface.

- **Rx and Tx Unsupported Codes:**

This field shows the number of OAMPDUs transmitted on this interface with an unsupported op-code.

- **Rx and Tx Link fault PDU's:**

This field shows the number of link fault PDUs received and transmitted on this interface.

- **Rx and Tx Dying Gasp:**

This field shows the number of dying gasp events received and transmitted on this interface.

- **Rx and Tx Critical Event PDU's:**

This field shows the number of critical event PDUs received and transmitted on this interface.

7.20 Ethernet OAM

Use the **Ethernet OAM** sub-menu to configure Connectivity Fault Management (CFM) Maintenance Entity Points (MEPs).

A domain is a section of a network that is under the responsibility of a single organization. MEPs are points in devices that participate in CFM at the edges of domains. Each domain has a maintenance level, so multiple domains may exist on the same device, provided the maintenance level is unique.

To configure the Ethernet OAM

1. Click **Configuration > Ethernet OAM**.
2. Click **Add new MEP**.
3. Configure the parameters.
4. Click **Save**.

Parameter description

- **Instance:**

Use this field to configure the identity of the MEP.

- **Domain:**

Use this drop-down box to configure the CFM domain. Possible values are:.

- **Port:** This is an MEP in the Port Domain. The Flow Instance is a Port.
- **Esp:** This is reserved for future use and needs a firmware upgrade to support it.
- **Evc:** This is an MEP in the EVC Domain. The Flow Instance is an EVC.
- **Mpls:** This is reserved for future use and needs a firmware upgrade to support it.

- **Mode:**

Use this drop-down box to configure this maintenance point as a **MEP** or **MIP** (Maintenance Intermediate Point).

- **Direction:**

Use this drop-down box to configure whether this maintenance point monitors **Ingress** or **Egress** traffic.

- **Residence Port:**

Use this field to configure which port this maintenance point monitors.

- **Level:**

Use this field to configure the Maintenance Entity Group (MEG) level of this maintenance point.

Shared MEGs don't encapsulate subscriber and service provider (SP) frames differently, so a pool of MEG levels are shared. The subscriber uses MEG levels 5 to 7 and the SP uses the remaining levels. When the encapsulation is different, the subscriber and SP can use all 8 levels.

- **Flow instance:**

Use this field to configure the MEP instance identifier for this flow. A MEP monitors a flow by sending periodic Continuity Check Messages (CCMs) for that flow.

- **Tagged VID:**

Use this field to configure an outer C/S-TAG depending on the VLAN Port Type (0 means no tag is added).

- **This MAC:**

This field shows the MEP device MAC address. This is used by other MEPs when unicast is selected.

- **Alarm:**

The shows the MEP alarm data. There is an active alarm on the MEP.

7.21 EPS

Use the **EPS** sub-menu to configure Ethernet Linear Protection Switching instances.

To configure Ethernet Linear Protection Switching:

1. Click **Configuration > EPS**.
2. Click **Add new EPS**.
3. Configure the parameters.
4. Click **Save**.

Parameter description

- **EPS ID:**

Use this field to configure the Ethernet Protection Switching identity.

- **Domain:**

Use this drop-down box to configure the CFM domain. Possible values are:.

- **Port:** This is an EPS instance in the Port Domain. The working/protected flow is a Port.
- **Esp:** This is reserved for future use and needs a firmware upgrade to support it.
- **Evc:** This is an EPS in the EVC Domain. The working/protected flow is an EVC.
- **Mpls:** This is reserved for future use and needs a firmware upgrade to support it.

- **Architecture:**

Use this field to configure a **1+1** or **1:1** EPS architecture.

- **W flow:**

Use this field to configure the working flow.

- **P flow:**

Use this field to configure the protecting flow.

- **W SF MEP:**

Use this field to configure the working Signal Fail reporting MEP.

- **P SF MEP:**

Use this field to configure the protecting Signal Fail reporting MEP.

- **APS MEP:**

Use this field to configure the APS PDU handling MEP.

- **Alarm:**

The shows the MEP alarm data. There is an active alarm on the MEP.

7.22 EPRS

Use the **EPRS** sub-menu to configure Ethernet Ring Protection Switching instances.

To configure Ethernet Ring Protection Switching:

1. Click **Configuration > EPRS**.
2. Click **Add new EPRS**.
3. Configure the parameters.
4. Click **Save**.

Parameter description

- **EPRS ID:**

Use this field to configure the Ethernet Ring Protection Switching identity.

- **Port 0:**

Use this field to configure port 0.

- **Port 1:**

Use this field to configure port 1. If the ring has only one connected port, configure this with **0** to disable it.

- **Port 0 SF MEP**

Use this field to configure port 0 Signal Fail reporting MEP.

- **Port 1 SF MEP**

Use this field to configure port 1 Signal Fail reporting MEP. If the ring has only one connected port, configure this with **0** to disable it.

- **Port 0 APS MEP**

Use this field to configure the port 0 APS PDU handling MEP.

- **Port 1 APS MEP**

Use this field to configure the port 1 APS PDU handling MEP. If the ring has only one connected port, configure this with **0** to disable it.

- **Ring Type:**

Use this field to configure the type of the protecting ring as a major ring or sub-ring.

- **Interconnected Node:**

Use this check box to configure this ring instance as interconnected or not interconnected.

- **Virtual Channel:**

Check this check box to configure a virtual channel for this sub-ring.

- **Major Ring ID:**

Use this field to configure the major ring group ID for the interconnected sub-ring. The major ring group ID is used to send topology changes on the major ring. For major rings, this value is the same as the protection group ID for this ring.

- **Alarm:**

The shows the MEP alarm data. There is an active alarm on the MEP.

Security

Chapter 8

8.1 Security

Use the **Security** menu to enhance the security of the LAN.

8.2 IP Source Guard

Use the **IP Source Guard** sub-menu to configure the switch to mitigate IP source address spoofing on the LAN.

8.2.1 Configuration

Use the **Configuration** sub-menu to enable IP Source Guard and limit the number of dynamic clients on a port-by-port basis.

To configure IP Source Guard:

1. Click **Security > IP Source Guard > Configuration**.
2. Configure the parameters.
3. Click **Save**.

Parameter description

IP Source Guard Configuration

- **Mode:**

Use this drop-down box to globally enable or disable IP Source Guard. All configured ACEs will be lost when the mode is enabled.

Port Mode Configuration

- **Port:**

This field shows the port number for this row.

- **Mode:**

Use this drop-down box to enable or disable IP Source Guard on this port.

- **Max Dynamic Clients:**

Use this drop-down box to configure a maximum of up to **3** dynamic clients that can be learned on this port. If this field is **0**, only packets with source addresses in the static table are forwarded via this port.

8.2.2 Static Table

Use the **Static Table** sub-menu to configure static IP source address to port mappings.

To configure the Static IP Source Guard Table:

1. Click **Security > IP Source Guard > Static Table**.
2. Click **Add new entry**.
3. Configure the parameters.
4. Click **Save**.

Parameter description

- **Port:**

Use this drop-down box to configure the port number for this row.

- **VLAN ID:**

Use this field to configure the VLAN ID for this row.

- **IP Address and IP Mask:**

Use these fields to configure the network of the source IP addresses allowed.

8.2.3 Dynamic Table

Use the **Dynamic Table** sub-menu to show the Dynamic IP Source Guard Table.

To show the Dynamic IP Source Guard Table, click **Security > IP Source Guard > Dynamic Table**.

Parameter description

- **Port:**

This field shows the port number for this row.

- **VLAN ID:**

This field shows the VLAN ID in which the IP traffic is permitted.

- **IP Address:**

This field shows the source IP addresses learned on this port.

- **MAC Address:**

This field shows the source MAC address associated with source IP addresses learned on this port.

8.3 ARP Inspection

Use the **ARP Inspection** sub-menu to configure the switch to ensure the IP address and MAC address in ARP packets is the same as those gleaned by snooping on DHCP packets.

8.3.1 Configuration

Use the **Configuration** sub-menu to enable ARP Inspection on a port-by-port basis.

To configure ARP Inspection:

1. Click **Security > ARP Inspection > Configuration**.
2. Configure the parameters.
3. Click **Save**.

Parameter description

ARP Inspection Configuration

- **Mode:**
Use this drop-down box to globally enable or disable ARP Inspection.

Port Mode Configuration

- **Port:**
This field shows the port number for this row.
- **Mode:**
Use this drop-down box to enable or disable ARP Inspection on this port.

8.3.2 Static Table

Use the **Static Table** sub-menu to configure static IP address to MAC address mappings that validate ARP packets.

To configure the Static ARP Inspection Table:

1. Click **Security > ARP Inspection > Configuration**.
2. Click **Add new entry**.
3. Configure the parameters.
4. Click **Save**.

Parameter description

- **Port:**

Use this drop-down box to configure the port number for this row.

- **VLAN ID:**

Use this field to configure the VLAN ID for this row.

- **MAC Address and IP Address:**

Use this field to configure the source MAC address to source IP address binding that is used to validate ARP request packets.

8.3.3 Dynamic Table

Use the **Dynamic Table** sub-menu to show the Dynamic ARP Inspection Table.

To show the Dynamic ARP Inspection Table, click **Security > ARP Inspection > Dynamic Table**.

Parameter description

- **Port:**

This field shows the port number for this row.

- **VLAN ID:**

This field shows the VLAN ID in which ARP traffic is permitted.

- **MAC Address:**

This field shows the source MAC address associated with source IP addresses learned on this port.

- **IP Address:**

This field shows the source IP addresses learned on this port.

8.4 DHCP Snooping

Use the **DHCP Snooping** sub-menu to prevent attackers from adding their own DHCP servers to the network.

8.4.1 Configuration

Use the **Configuration** sub-menu to enable DHCP Snooping on a port-by-port basis.

To configure DHCP Snooping

1. Click **Security > DHCP Snooping > Configuration**.
2. Configure the parameters.
3. Click **Save**.

Parameter description

DHCP Snooping Configuration

- **Mode:**

Use this drop-down box to globally enable or disable DHCP Snooping.

Port Mode Configuration

- **Port:**

This field shows the port number for this row.

- **Mode:**

Use this drop-down box to configure this port as a **Trusted** or **Untrusted**. DHCP request messages are forwarded to trusted ports and DHCP replies are only accepted from trusted ports.

8.4.2 Statistics

Use the **Statistics** sub-menu to show DHCP Snooping statistics on a port-by-port basis.

To show DHCP Snooping statistics:

1. Click **Security > DHCP Snooping > Statistics**.
2. Choose a port number from the port drop-down box next to the **Auto-refresh** check box.

Parameter description

- **Rx and Tx Discover:**

This field shows the number of discover (option 53 with value 1) packets received and transmitted.

- **Rx and Tx Offer:**

This field shows the number of offer (option 53 with value 2) packets received and transmitted.

- **Rx and Tx Request:**

This field shows the number of request (option 53 with value 3) packets received and transmitted.

- **Rx and Tx Decline:**

This field shows the number of decline (option 53 with value 4) packets received and transmitted.

- **Rx and Tx ACK:**

This field shows the number of ACK (option 53 with value 5) packets received and transmitted.

- **Rx and Tx NAK:**

This field shows the number of NAK (option 53 with value 6) packets received and transmitted.

- **Rx and Tx Release:**

This field shows the number of release (option 53 with value 7) packets received and transmitted.

- **Rx and Tx Inform:**

This field shows the number of inform (option 53 with value 8) packets received and transmitted.

- **Rx and Tx Lease Query:**

This field shows the number of lease query (option 53 with value 10) packets received and transmitted.

- **Rx and Tx Lease Unassigned:**

This field shows the number of lease unassigned (option 53 with value 11) packets received and transmitted.

- **Rx and Tx Lease Unknown:**

This field shows the number of lease unknown (option 53 with value 12) packets received and transmitted.

- **Rx and Tx Lease Active:**

This field shows the number of lease active (option 53 with value 13) packets received and transmitted.

8.5 DHCP Relay

Use the **DHCP Relay** sub-menu to configure the switch to forward DHCP requests to a DHCP server on another network and drop DHCP broadcasts.

8.5.1 Configuration

Use the Configuration sub-menu to define how DHCP packets are relayed.:

To configure DHCP Relay:

1. Click **Security > DHCP Relay > Configuration**.
2. Configure the parameters.
3. Click **Save**.

Parameter description

- **Relay Mode:**
Use this drop-down box to **Enable** or **Disable** DHCP relay.
- **Relay Server:**
Use this field to configure the IP address of the DHCP server.
- **Relay Information Mode:**
Use this drop-down box to configure whether option 82 is inserted into forwarded DHCP messages and removed from DHCP messages forwarded to DHCP clients.
- **Relay Information Policy:**
Use this drop-down box to configure whether to **Replace** or **Keep** relay agent information in messages that already have this information, or **Drop** such DHCP packets.

8.5.2 Statistics

Use the **Statistics** sub-menu to show DHCP Relay statistics.

To show DHCP Relay statistics, click **Security > DHCP Relay > Statistics**.

Parameter description

Server Statistics

- **Transmit to Server:**

This field shows the number of packets that have been relayed from clients to the server.

- **Transmit Error:**

This field shows the number of packets that resulted in errors while being sent to clients.

- **Receive from Server:**

This field shows the number of packets received from the server.

- **Receive Missing Agent Option:**

This field shows the number of packets received without agent information options.

- **Receive Missing Circuit ID:**

This field shows the number of packets received with the Circuit ID option missing.

- **Receive Missing Remote ID:**

This field shows the number of packets received with the Remote ID option missing.

- **Receive Bad Circuit ID:**

This field shows the number of packets whose Circuit ID option didn't match a known circuit ID.

- **Receive Bad Remote ID:**

This field shows the number of packets whose Remote ID option didn't match a known Remote ID.

Client Statistics

- **Transmit to Client:**

This field shows the number of packets that have been relayed from the server to clients.

- **Transmit Error:**

This field shows the number of packets that resulted in error while being sent to clients.

- **Receive from Client:**

This field shows the number of packets received from clients.

- **Receive Agent Option:**

This field shows the number of packets received with the relay agent information option.

- **Replace Agent Option:**

This field shows the number of packets that had their relay agent information option replaced.

- **Keep Agent Option:**

This field shows the number of packets whose relay agent information was retained.

- **Drop Agent Option:**

This field shows the number of packets that were dropped for containing relay agent information.

8.6 NAS

Use the **NAS** sub-menu to configure the Network Access Server. NAS is used to authenticate users on a port-by-port basis.

8.6.1 Configuration

Use the **Configuration** sub-menu to setup NAS globally and on a port-by-port basis.

To configure NAS:

1. Click **Security > NAS > Configuration**.
2. Configure the parameters.
3. Click **Save**.

Parameter description

System Configuration

- **Mode:**

Use this drop-down box to globally enable or disable NAS.

- **Reauthentication Enabled and Reauthentication Period:**

Check this check box to reauthenticate authenticated supplicants/clients after the interval specified by **Reauthentication Period (1 to 3600 seconds)**. The Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.

For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).

- **EAPOL Timeout:**

Use this field to configure the retransmission time (**1 to 255 seconds**) for Request Identity EAPOL frames. This has no effect for MAC-based ports.

- **Aging Period:**

Use this field to configure the time (**10** to **1000000** seconds) after which authenticated MAC address entries are deleted. This field applies to the Single 802.1X, Multi 802.1X and MAC-Based Auth modes that use Port Security to secure MAC addresses.

When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module checks for activity on the MAC address and frees resources if no activity is seen within the aging period.

If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.

For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

- **Hold Time:**

Use this field to configure how long a client that fails authentication must remain locked out before being allowed to authenticate. This field can be between **10** and **1000000** seconds and applies to the Single 802.1X, Multi 802.1X and MAC-Based Auth modes that use Port Security to secure MAC addresses.

If a client fails to authenticate because the RADIUS server denies the client access or because the RADIUS server request times out, the client is put on hold in the Unauthorized state. The hold timer pauses during authentication.

In MAC-based authentication mode, the switch ignores frames from the client during the hold time.

- **RADIUS-Assigned QoS Enabled:**

Use this check box to globally enable a RADIUS server to assign a QoS class to authenticated supplicants.

This enables central control of the traffic class applied to traffic from an authenticated supplicant. The RADIUS server must also be configured to transmit special RADIUS attributes to take advantage of this feature.

- **RADIUS-Assigned VLAN Enabled:**

Use this check box to globally enable a RADIUS server to assign a VLAN to authenticated supplicants.

This enables central control of the VLAN an authenticated supplicant is a member of.

The RADIUS server must also be configured to transmit special RADIUS attributes to take advantage of this feature.

- **Guest VLAN Enabled:**

Use this check box to globally enable 802.1X-unaware clients to be made members of the guest VLAN after an administrator-defined time-out.

- **Guest VLAN ID:**

Use this field to configure the guest VLAN ID.

- **Max. Reauth. Count:**

Use this field to configure the number of times (1 to 255) the switch transmits an EAPOL Request Identity frame without response before moving the client to the guest VLAN.

- **Allow Guest VLAN if EAPOL Seen:**

Use this check box to globally enable clients to be made members of the guest VLAN even if an EAPOL frame has been received on the port to which the client is connected at any time during the lifetime of the port. If this check box is unchecked (default), the client only becomes a member of the Guest VLAN if an EAPOL frame has not been received on the port to which the client is connected at any time during the lifetime of the port.

Port Mode Configuration

- **Port:**

This field shows the port number for this row.

- **Admin State:**

If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:

- **Force Authorized:** In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.
- **Force Unauthorized:** In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.
- **Port-based 802.1X:** In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it. When authentication is

complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Note:

Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

- **Single 802.1X:** In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.
- **Multi 802.1X:** In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Multi 802.1X variant. Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module. In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any

suplicants that might be on the port. The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

- **MAC-based Auth.:** Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both user-name and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string in the following form xx-xx-xx-xx-xx-xx, that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard. The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

- **RADIUS-Assigned QoS Enabled:**

When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class immediately reverts to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned QoS Class). This option is only available for Port-based 802.1X and Single 802.1X modes.

RADIUS attributes used in identifying a QoS Class

Refer to the written documentation for a description of the RADIUS attributes needed in order to successfully identify a QoS Class. The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet. Only the first occurrence of the attribute in the packet will be considered, and to be valid all 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' to '3', which translates into the desired QoS Class in the range 0 to 3.

- **RADIUS-Assigned VLAN Enabled:**

When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID. If (re-)authentication fails, the RADIUS Access-Accept packet no longer carries a valid VLAN ID or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned VLAN ID). This option is only available for Port-based 802.1X and Single 802.1X modes. To troubleshoot VLAN assignments, use the **Configuration > VLAN > VLAN Membership** and **Port Status** sub-menus to see which modules have (temporarily) overridden the current port VLAN configuration.

RADIUS attributes used in identifying a VLAN ID

RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

- The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.
- The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):
 - Value of Tunnel-Medium-Type must be set to IEEE-802 (ordinal 6).
 - Value of Tunnel-Type must be set to VLAN (ordinal 13).
 - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].

- **Guest VLAN Enabled:**

When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below.

This option is only available for EAPOL-based modes, i.e.:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

To troubleshoot VLAN assignments, use the **Configuration > VLAN > VLAN Membership** and **Port Status** sub-menus to see which modules have (temporarily) overridden the current port VLAN configuration.

Guest VLAN Operation

When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.

While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the Allow Guest VLAN if EAPOL Seen is disabled.

- **Port State:**

This field shows one of the following port states:

- **Globally Disabled:** NAS is globally disabled.
- **Link Down:** NAS is globally enabled, but there is no link on the port.
- **Authorized:** The port is in Force Authorized or a single-suppliant mode and the supplicant is authorized.
- **Unauthorized:** The port is in Force Unauthorized or a single-suppliant mode and the supplicant is not successfully authorized by the RADIUS server.
- **X Auth/Y Unauth:** The port is in a multi-suppliant mode. Currently X clients are authorized and Y are unauthorized.

- **Restart:**

Click one of the following buttons to reauthenticate or reinitialize the port:

- **Reauthenticate:** Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. This button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.
- **Reinitialize:** Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

These buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect.

8.6.2 Switch Status

Use the **Switch Status** sub-menu to show the NAS status of all ports.

To show NAS Switch Status, click **Security > NAS > Switch Status**.

Parameter description

- **Port:**

This field shows the port number for this row. Click the port number to show detailed NAS statistics for this port.

- **Admin State:**

This field shows the port's current administrative state. Refer to NAS Admin State for a description of possible values.

- **Port State:**

This field shows the current state of the port. Refer to NAS Port State for a description of the individual states.

- **Last Source:**

This field shows the source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

- **Last ID:**

This field shows the user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

- **QoS Class:**

This field shows the QoS Class assigned to the port by the RADIUS server if enabled.

- **Port VLAN ID:**

This field shows the VLAN ID that the NAS has put the port in. The field is blank if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, **(RADIUS-assigned)** is appended to the VLAN ID. If the port is moved to the Guest VLAN, **(Guest)** is appended to the VLAN ID.

8.6.3 Port Status

Use the **Port Status** sub-menu to show NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication.

To show NAS Port Status:

1. Click **Security > NAS > Port Status**.
2. Select the port number from the Port Index drop-down box to show detailed port statistics for that port.

Parameter description

Port State

- **Admin State:**

This field shows the port's current administrative state.

- **Port State:**

This field shows the current state of the port.

- **QoS Class:**

This field shows the QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.

- **Port VLAN ID:**

This field shows the VLAN ID that the NAS has put the port in. The field is blank if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, **(RADIUS-assigned)** is appended to the VLAN ID. If the port is moved to the Guest VLAN, **(Guest)** is appended to the VLAN ID.

Port Counters

- **EAPOL Counters:**

These supplicant frame counters are available for the Force Authorized, Force Unauthorized, Port-based 802.1X, Single 802.1X and Multi 802.1X administrative states.

- **Backend Server Counters:**

These backend (RADIUS) frame counters are available for the Port-based 802.1X, Single 802.1X, Multi 802.1X, MAC-based Auth administrative states.

- **Last Supplicant/Client Info:**

Information about the last supplicant/client that attempted to authenticate. This information is available for the Port-based 802.1X, Single 802.1X, Multi 802.1X and MAC-based Auth administrative states.

- **Selected Counters:**

The Selected Counters table is visible when the port is in the Multi 802.1X or MAC-based Auth administrative state. The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the Attached MAC Addresses from the table below.

Attached MAC Addresses

- **Identity:**

This field shows the identity of the supplicant, as received in the Response Identity EAPOL frame. Clicking an identity causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows **No supplicants attached**. This column is not available for MAC-based Auth.

- **MAC Address:**

This field shows the MAC address of the attached supplicant for Multi 802.1X mode. In MAC-based Auth mode, this column holds the MAC address of the attached client. Clicking a MAC address causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows **No clients attached**.

- **VLAN ID:**

This field shows the VLAN ID of the corresponding client as determined by the Port Security module.

- **State:**

This field shows the authentication state of the client. In the authenticated state, the client's frames are forwarded on the port, and in the unauthenticated state, they're blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails, the client remains in the unauthenticated state for Hold Time seconds.

- **Last Authentication:**

This field shows the date and time of the last successful or unsuccessful authentication of the client.

8.7 AAA

Use the **AAA** sub-menu to configure a TACACS+ or RADIUS AAA (Authentication, Authorization, Accounting) server to provide access control for the network. The AAA server can be a server.

8.7.1 Configuration

Use the **Configuration** sub-menu to setup an authentication server for the switch.

To configure an authentication server:

1. Click **Security > AAA > Configuration**.
2. Configure the parameters.
3. Click **Save**.

Parameter description

Common Server Configuration

- **Timeout:**

The Timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server. If the server does not reply within this timeframe, we will consider it to be dead and continue with the next enabled server (if any). RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.

- **Dead Time:**

The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

TACACS+ Authorization and Accounting Configuration

- **Authorization**

Use this drop-down box to **Enable** or **Disable** TACACS+ authorization on this switch.

- **Fallback to Local Authorization**

Use this drop-down box to configure whether the switch uses local authentication if TACACS+ authorization is not available.

- **Accounting**

Use this drop-down box to **Enable** or **Disable** TACACS+ accounting on this switch

RADIUS Authentication Server Configuration

- **#:**

The RADIUS Authentication Server number for which the configuration below applies.

- **Enabled:**

Enable the RADIUS Authentication Server by checking this box.

- **IP Address/Host name:**

The IP address or host name of the RADIUS Authentication Server.

- **Port:**

The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server.

- **Secret:**

The secret - up to 29 characters long - shared between the RADIUS Authentication Server and the switch stack.

RADIUS Accounting Server Configuration

The table has one row for each RADIUS Accounting Server and a number of columns, which are:

- **#:**

The RADIUS Accounting Server number for which the configuration below applies.

- **Enabled:**

Enable the RADIUS Accounting Server by checking this box.

- **IP Address/Host name:**

The IP address or host name of the RADIUS Accounting Server. IP address is expressed in dotted decimal notation.

- **Port:**

The UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server.

- **Secret:**

The secret - up to 29 characters long - shared between the RADIUS Accounting Server and the switch stack.

TACACS+ Authentication Server Configuration

The table has one row for each TACACS+ Authentication Server and a number of columns, which are:

- **#:**

The TACACS+ Authentication Server number for which the configuration below applies.

- **Enabled:**

Enable the TACACS+ Authentication Server by checking this box.

- **IP Address/Host name:**

The IP address or host name of the TACACS+ Authentication Server. IP address is expressed in dotted decimal notation.

- **Port:**

The TCP port to use on the TACACS+ Authentication Server. If the port is set to 0 (zero), the default port (49) is used on the TACACS+ Authentication Server.

- **Secret:**

The secret - up to 29 characters long - shared between the TACACS+ Authentication Server and the switch stack.

8.7.2 RADIUS Overview

Use the **RADIUS Overview** sub-menu to check that the RADIUS Authentication and Accounting servers are available.

To show RADIUS Overview, Click **Security > AAA > Radius Overview**.

Parameter description

- **#:**
The RADIUS server number. Click to navigate to detailed statistics for this server.
- **IP Address:**
The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
- **State:**
The current state of the server. This field takes one of the following values:
 - **Disabled:** The server is disabled.
 - **Not Ready:** The server is enabled, but IP communication is not yet up and running.
 - **Ready:** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.
 - **Dead (X seconds left):** Accounting/Authentication attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

8.7.3 RADIUS Details

Use the **RADIUS Details** sub-menu to show statistics on the RADIUS Authentication and Accounting servers. The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.

To show RADIUS server statistics:

1. Click **Configuration > Port > RADIUS Details**.
2. Select the server number from the Server Number drop-down box to show detailed statistics for that server.

Parameter description

RADIUS Authentication Statistics

These statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.

Packet Counters

- **Access Accepts:**
The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
- **Access Rejects:**
The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
- **Access Challenges:**
The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
- **Malformed Access Responses:**
The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
- **Bad Authenticators:**
The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
- **Unknown Types:**

The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.

- **Packets Dropped:**

The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.

- **Access Requests:**

The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.

- **Access Retransmissions:**

The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.

- **Pending Requests:**

The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.

- **Timeouts:**

The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

- **State:**

The current state of the server. This field takes one of the following values:

- **Disabled:** The server is disabled.

- **Not Ready:** The server is enabled, but IP communication is not yet up and running.

- **Ready:** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.

- **Dead (X seconds left):** Accounting/Authentication attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

- **Round-Trip Time:**

The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Statistics

- **Responses:**

The number of RADIUS packets (valid or invalid) received from the server.

- **Malformed Responses:**

The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.

- **Bad Authenticators:**

The number of RADIUS packets containing invalid authenticators received from the server.

- **Unknown Types:**

The number of RADIUS packets of unknown types that were received from the server on the accounting port.

- **Packets Dropped:**

The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.

- **Requests:**

The number of RADIUS packets sent to the server. This does not include retransmissions.

- **Retransmissions:**

The number of RADIUS packets retransmitted to the RADIUS accounting server.

- **Pending Requests:**

The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.

- **Timeouts:**

The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

- **Timeouts:**

The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

- **State:**

The current state of the server. This field takes one of the following values:

- **Disabled:** The server is disabled.
- **Not Ready:** The server is enabled, but IP communication is not yet up and running.
- **Ready:** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.
- **Dead (X seconds left):** Accounting/Authentication attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

- **Round-Trip Time:**

The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

8.8 Port Security

Use the **Port Security** sub-menu to restrict input to an interface by restricting connections by source MAC address.

8.8.1 Limit Control

Use **Limit Control** to configure how MAC addresses are restricted on a port-by-port basis.

To configure a System Configuration of Limit Control

1. Click **Security > Port Security > Limit Control**.
2. Configure the parameters.
3. Click **Save**.

Parameter description

System Configuration

- **Mode:**

Indicates if Limit Control is globally enabled or disabled on the switch stack. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

- **Aging Enabled:**

If checked, secured MAC addresses are subject to aging as discussed under Aging Period.

- **Aging Period:**

If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.

The Aging Period can be set to a number between 10 and 10,000,000 seconds.

To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Port Configuration

- **Port:**

The port number to which the configuration below applies.

- **Mode:**

Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.

- **Limit:**

The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.

The switch is born with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

- **Action:**

If Limit is reached, the switch can take one of the following actions:

- **None:** Do not allow more than Limit MAC addresses on the port, but take no further action.
- **Trap:** If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded.
- **Shutdown:** If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:
 - Boot the stack or elect a new master the switch,
 - Disable and re-enable Limit Control on the port or the stacks witch,

- Click the Reopen button.
- **Trap & Shutdown:** If Limit + 1 MAC addresses is seen on the port, both the Trap and the Shutdown actions described above will be taken.
- **State:**
This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values:
 - **Disabled:** Limit Control is either globally disabled or disabled on the port.
 - **Ready:** The limit is not yet reached. This can be shown for all actions.
 - **Limit Reached:** Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap.
 - **Shutdown:** Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.
- **Re-open Button:**

If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to Shutdown in the Action section.

Note:

Clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost

8.8.2 Switch Status

Use the **Switch Status** sub-menu to show the overall state of Port Security.

Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise. The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

To show Port Security Switch Status, click **Security > Port Security > Switch Status**.

Parameter description

User Module Legend

This shows all user modules that may request Port Security services.

- **User Module Name:**

The full name of a module that may request Port Security services.

- **Abbr:**

A one-letter abbreviation of the user module. This is used in the Users column in the port status table.

Port Status

- **Port:**

The port number for which the status applies. Click the port number to see the status for this particular port.

- **Users:**

Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.

- **State:**

Shows the current state of the port. It can take one of four values:

- **Disabled:** No user modules are currently using the Port Security service.
- **Ready:** The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.
- **Limit Reached:** The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.
- **Shutdown:** The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.

- **MAC Count (Current, Limit):**

These two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.

If no user modules are enabled on the port, the **Current** column will show a dash (-).

If the Limit Control user module is not enabled on the port, the **Limit** column will show a dash (-).

Indicates the number of currently learned MAC addresses (forwarding as well as blocked) on the port. If no user modules are enabled on the port, a dash (-) will be shown.

8.8.3 Port Status

Use the **Port Status** sub-menu to show the MAC addresses secured by the Port Security module on a port-by-port basis.

Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

To show Port Security Port Status:

1. Click **Security > Port Security > Port Status**.
2. Select the port number from the Port Number drop-down box to show the state of that port.

Parameter description

- **MAC Address & VLAN ID:**

The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating No MAC addresses attached is displayed.

- **State:**

Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.

- **Time of Addition:**

Shows the date and time when this MAC address was first seen on the port.

- **Age/Hold:**

If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin.

If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

8.9 Access Management

Use the **Access Management** sub-menu to configure which protocol can be used to manage the switch.

8.9.1 Configuration

Use the **Configuration** sub-menu to setup which protocols and IP addresses can be used to manage the switch. Up to 16 access rules can be configured.

To configure Access Management.

1. Click **Security > Access Management > Configuration**.
2. Click **Add new entry**.
3. Configure the parameters.
4. Click **Save**.

Parameter description

- **Mode:**

Use this drop-down box to **Enable** or **Disable** access management.

- **Start IP address:**

Indicates the start IP address for the access management entry.

- **End IP address:**

Indicates the end IP address for the access management entry.

- **HTTP/HTTPS:**

Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.

- **SNMP:**

Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.

- **TELNET/SSH:**

Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

8.9.2 Statistics

Use the **Statistics** sub-menu to show Access Management statistics.

To show Access Management statistics, click **Security > Access Management > Statistics**.

Parameter description

- **Interface:**

The interface type through which the remote host can access the switch.

- **Received Packets:**

Number of received packets from the interface when access management mode is enabled.

- **Allowed Packets:**

Number of allowed packets from the interface when access management mode is enabled

- **Discarded Packets:**

Number of discarded packets from the interface when access management mode is enabled.

8.10 SSH

Use the **SSH** sub menu to enable this switch to be managed via the SSH (Secure SHell) protocol. SSH combines authentication and data encryption to provide secure encrypted communication.

To configure SSH, click **Security > SSH**.

Parameter description

- **Mode:**

Use this drop-down box to **Enable** or **Disable** SSH.

- **Buttons:**

Save - Click to save changes.

Reset - Click to undo any changes made locally and revert to previously saved values.

8.11 HTTPS

Use the **HTTPS** sub menu to enable this switch to be managed via the **HTTPS** (HTTP Secure) protocol. HTTPS combines authentication and data encryption to provide secure encrypted communication.

To configure HTTPS, click **Security > HTTPS**.

Parameter description

- **Mode:**

Use this drop-down box to **Enable** or **Disable** HTTPS.

- **Automatic Redirect:**

Use this drop-down box to **Enable** or **Disable** HTTPS automatically redirect web browsers to HTTPS when HTTPS mode is enabled.

8.12 AUTH Method

Use the **AUTH Method** sub-menu to configure how client is authenticated when logging into one of the management interfaces.

To configure an Authentication Method:

1. Click **Security > AUTH Method**.
2. Configure the parameters.
3. Click **Save**.

Parameter description

- **Client:**

The management client for which the configuration below applies.

- **Authentication Method:**

Authentication Method can be set to one of the following values:

- **none:** authentication is disabled and login is not possible.
- **local:** use the local user database on the switch stack for authentication.
- **RADIUS:** use a remote RADIUS server for authentication.
- **TACACS+:** use a remote TACACS+ server for authentication.

- **Fallback:**

Check this check box to enable fallback to local authentication. If none of the configured authentication servers are available, the local user database is used for authentication. This is only possible if the Authentication Method is set to a value other than none or local.

Maintenance

Chapter 9

Use the Maintenance menu to restart the switch, upgrade the firmware; save, restore, import or export switch configuration; or perform network diagnostics.

9.1 Restart Device

Use the Restart Device sub-menu to reboot the switch.

To restart the switch, click **Maintenance > Restart Device**, and follow the onscreen prompts.

9.2 Firmware

Use the **Firmware** sub-menu to upgrade the firmware or revert to the previous version of firmware. The switch can be enhanced with more features by installing firmware upgrades.

9.2.1 Firmware Upgrade

Use the **Firmware Upgrade** sub-menu to upgrade the firmware.

To upgrade the firmware,

1. Click **Maintenance > Firmware > Firmware Upgrade**.
2. Browse to the new firmware file.
3. Click **Upload** to upload the firmware file to the switch.
4. Follow the onscreen prompts to complete the firmware upgrade.

Note:

This page facilitates an update of the firmware controlling the stack. switch. Uploading software will update all managed switches in the stack to the location of a software image and click. After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and all managed switches in the stack restart. the switch restarts.

WARNING:

While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time or the switch may fail to function afterwards.

9.2.2 Firmware Selection

Use the **Firmware Selection** sub-menu to revert to the previous version of firmware.

To revert to a previous firmware version:

1. Click **Maintenance > Firmware > Firmware Selection**.
2. Click **Activate Alternate Image**.
3. Follow the onscreen prompts to complete the firmware reversion.

Parameter description

- **Activate Alternate Image:**

Click to use the alternate image. This button may be disabled depending on system state.

- **Cancel:**

Cancel activating the backup image. Navigates away from this page.

- **Image:**

The flash index name of the firmware image. The name of primary (preferred) image is image, the alternate image is named image.bk.

- **Version:**

The version of the firmware image.

- **Date:**

The date where the firmware was produced.

Note:

In case the active firmware image is the alternate image, only the Active Image table is shown. In this case, the Activate Alternate Image button is also disabled.

If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.

The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

9.3 Save/Restore

Use the **Save/Restore** sub-menu to save or restore the switch configuration.

9.3.1 Factory Defaults

Use the **Factory Defaults** sub-menu to reset the switch configuration to the same as it was when manufactured.

To reset the switch to factory default configuration:

1. Click **Maintenance > Save/Restore > Factory Defaults**.
2. Follow the onscreen prompts to complete the process.

9.3.2 Save Start

Use the **Save Start** sub-menu to save the switch's configuration, so this configuration is used after a power cycle.

To save the configuration:

1. Click **Maintenance > Save/Restore > Save Start**.
2. Follow the onscreen prompts to complete the process.

9.3.3 Save User

Use the **Save User** sub-menu to save the switch's configuration to the backup user part of the flash memory.

To save the configuration:

1. Click **Maintenance > Save/Restore > Save User**.
2. Follow the onscreen prompts to complete the process.

9.3.4 Restore User

Use the **Restore User** sub-menu to restore the switch's configuration from the backup user part of the flash memory.

To restore the configuration:

1. Click **Maintenance > Save/Restore > Restore User**.
2. Follow the onscreen prompts to complete the process.

9.4 Export/Import

Use the **Export/Import** sub-menu to export or import the switch configuration to an XML file.

9.4.1 Export Config

Use the **Export Config** sub-menu to save the switch's configuration to an XML file.

To save the configuration:

1. Click **Maintenance > Export/Import > Export Config**.
2. Follow the onscreen prompts to complete the process.

9.4.2 Import Config

Use the **Import Config** sub-menu to import the switch's configuration from an XML file.

To import the configuration:

1. Click **Maintenance > Export/Import > Import Config**.
2. Browse to the new configuration file.
3. Click **Upload** to upload the configuration file to the switch.
4. Follow the onscreen prompts to complete the process.

9.5 Diagnostics

Use the **Diagnostics** sub-menu to perform basic network diagnostics.

9.5.1 Ping

Use the **Ping** sub-menu to execute an ICMP ping from the switch's management interface.

To start an ICMP ping:

1. Click **Maintenance > Diagnostics > Ping**.
2. Configure the parameters.
3. Click **Start**.

Parameter description

- **IP Address:**

Use this field to configure the IP address of the host to ping.

- **Ping Size:**

Use this field to configure the ICMP packet size.

9.5.2 Ping6

Use the **Ping6** sub-menu to execute an ICMPv6 ping from the switch's management interface.

To start an ICMP ping:

1. Click **Maintenance > Diagnostics > Ping6**.
2. Configure the parameters.
3. Click **Start**.

Parameter description

- **IP Address:**

Use this field to configure the IPv6 address of the host to ping.

- **Ping Size:**

Use this field to configure an ICMPv6 payload size from 8 bytes to 1400 bytes.

Part III: Front Matter

Front Matter

Chapter 10

10.1 Power, Hardware Connections and LEDs

The switch does not turn on. None of the LEDs turn on.

1. Make sure the switch is turned on (in DC models or if the DC power supply is connected in AC/DC models).
2. Make sure you are using the power adaptor or cord included with the switch.
3. Make sure the power adaptor or cord is connected to the switch and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the switch off and on (in DC models or if the DC power supply is connected in AC/DC models).
5. Disconnect and re-connect the power adaptor or cord to the switch (in AC models or if the AC power supply is connected in AC/DC models).
6. If the problem continues, contact the vendor.

The ALM LED is on.

1. Turn the switch off and on (in DC models or if the DC power supply is connected in AC/DC models).
2. Disconnect and re-connect the power adaptor or cord to the switch (in AC models or if the AC power supply is connected in AC/DC models).
3. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See “LEDs” on page 13.
2. Check the hardware connections. See “Front Panel Connections” on page 2.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the switch off and on (in DC models or if the DC power supply is connected in AC/DC models).
5. Disconnect and re-connect the power adaptor or cord to the switch (in AC models or if the AC power supply is connected in AC/DC models).
6. If the problem continues, contact the vendor.

10.2 Switch Access and Login

I forgot the IP address for the switch.

1. The default in-band IP address is **192.168.1.1**.
2. Use the console port to log in to the switch.
3. Use the **MGMT** port to log in to the switch, the default IP address of the **MGMT** port is 192.168.0.1.
4. If this does not work, you have to reset the device to its factory defaults. See “Factory Defaults” on page 5.

I forgot the user name and/or password.

1. The default user name is **admin** and the default password is empty.
2. If this does not work, you have to reset the device to its factory defaults. See “Factory Defaults” on page 5.

I cannot see or access the Login screen in the web configurator.

1. Make sure you are using the correct IP address.
 - The default in-band IP address is 192.168.1.1.
 - If you changed the IP address, use the new IP address.
 - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the switch.
2. Check the hardware connections, and make sure the LEDs are behaving as expected. See “LEDs” on page 13.
3. Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled.
4. Make sure your computer is in the same subnet as the switch. If you know that there are routers between your computer and the switch, skip this step.
5. Reset the device to its factory defaults, and try to access the switch with the default IP address. See “Factory Defaults” on page 5.
6. If the problem continues, contact the vendor, or try one of the advanced suggestions.

Advanced Suggestions

Try to access the switch using another service, such as Telnet. If you can access the switch, check the remote management settings to find out why the switch does not respond to HTTP.

I can see the Login screen, but I cannot log in to the switch.

1. Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is empty. These fields are case sensitive, so make sure [Caps Lock] is not on.
2. You may have exceeded the maximum number of concurrent Telnet sessions. Close other Telnet session(s) or try connecting again later. Check that you have enabled logins for HTTP or Telnet. If you have configured a secured client IP address, your computer's IP address must match it. See "Access Management" on page 40.
3. Disconnect and re-connect the cord to the switch.
4. If this does not work, you have to reset the device to its factory defaults. See "Factory Defaults" on page 5.

Pop-up Windows, JavaScript and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

I cannot see some of the submenus at the bottom of the navigation panel.

The recommended screen resolution is 1024 by 768 pixels. Adjust the value in your computer and then you should see the rest of the submenus at the bottom of the navigation panel.

There is unauthorized access to my switch via telnet, HTTP and SSH.

Click **System > Syslog > Log** to check for unauthorized access to your switch. To avoid unauthorized access, click **Security > Access Management > Configuration** and limit the range of IP addresses allowed access to trusted hosts. See "Access Management" on page 40. Computers with IP addresses outside permitted ranges cannot access the management interface of the switch.

10.3 Switch Configuration

I lost my configuration settings after I restarted the switch.

Make sure you save your configuration into the switch's nonvolatile memory each time you make changes. Click **Maintenance > Save/Restore > Save Start** to save the configuration permanently. See "Save/Restore" on page 5.

Front Matter

Chapter 11

11.1 Hardware Specifications

The following tables summarize the switch's hardware features.

Key Features

Table 11-1: Key Features

SPECIFICATION	DESCRIPTION
CPU	400 MHz MIPS CPU
MAC chip	Vitesse VSC7460
PHY chip	Vitesse VSC8488 for 10G SFP+ (XGS3600-26F only) Vitesse VSC8664 for 4-port dual personality GbE RJ-45/SFP
RAM	DDR2 128 MB (64 M x 16)
Flash	32 MB (16 MB SPI x 2), dual image support
Packet buffer size	4 MB
MAC table	32 K
Switching capacity	14880 pps at 10 Mbps 148810 pps at 100 Mbps 1488095 pps at 1 Gbps with 64-byte packets
Total switch capacity	88 Gbps
Forwarding rate	50.5 Mpps

Interface

Table 11-2: Interface

SPECIFICATION	DESCRIPTION
Uplink interfaces (XGS3600-26F only)	Fixed uplink 2 x 10 Gigabit ports (1/10 Gb SFP+)
Subscriber interfaces	20 x Gigabit ports (single 100/1000 Mb SFP port) 4 x Dual personality interfaces (10/100/1000Base-T RJ-45 port & 100/1000 Mb SFP port) Auto-negotiation Auto-MDIX
Management interface	1 x Out-of-band management port (10/100/1000Base-T)
Standards	IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX Ethernet IEEE 802.3ab 1000Base-T Ethernet IEEE 802.3z 1000Base-X Ethernet IEEE 802.3x flow control IEEE 802.3az Energy Efficient Ethernet support (only RJ-45 interfaces) IEEE 802.1p CoS support

LED Indicators

Table 11-3: LED Indicators

SPECIFICATION	DESCRIPTION
System LED	<p>Steady green: boot up successful</p> <p>Flash green: boot up in process</p> <p>Unlit: power off or boot up failed</p>
Alarm LED	<p>Steady red: system failure because of overheating, wrong voltage or abnormal fan speed</p> <p>Unlit: switch is in normal condition</p>
Power LED	<p>Steady green: power on</p> <p>Unlit: power off or fail</p>
Backup power LED	<p>Steady green: power on</p> <p>Unlit: power off or fail</p>
SFP LED (P1 - 24)	<p>Steady green: 1000 Mbps link-up</p> <p>Steady amber: 100 Mbps link-up</p> <p>Flash green/yellow: activity (receiving or transmitting data)</p> <p>Unlit green/amber: port disconnected or link failed</p>

Table 11-3: LED Indicators

SPECIFICATION	DESCRIPTION
RJ-45 LED (P21 - 24)	Steady green: 1000 Mbps link-up Steady amber: 100 Mbps link-up Flash green/amber: activity (receiving or transmitting data) Unlit green/amber: port disconnected or link failed
SFP+ LED (P25 - 26) (XGS3600-26F only)	Steady green: 1 Gbps link-up Steady amber: 10 Gbps link-up Flash green/amber: activity (receiving or transmitting data) Unlit green/amber: port disconnected or link failed

General

Table 11-4: General

SPECIFICATION	DESCRIPTION
Console port	Female D-sub 9 pin (DCE)
Fan design	Three fans on the rear panel. One fan is dedicated to the power supply.
Reset button	Push button accessed through right-hand ventilation slots
Dimensions	19", 1U High, 442 x 211 x 44mm (W x D x H)
Weight	TBD

Table 11-4: General

SPECIFICATION	DESCRIPTION
Temperature	Operating: 0 ~ 60°C Storage: -20 ~ 70°C
Operating humidity	5 ~ 90% non-condensing
System monitoring	AC power supply internal 12-volt output DC power supply internal 12-volt output 3 fan speed sensors 2 temperature sensors
Dying gasp	
Power supply	Redundant 85 W AC and DC power inputs: <ul style="list-style-type: none"> <li data-bbox="698 822 1989 861">■ 100 ~ 240 V AC in (via 3-pin socket); 12 V, 5 A minimum out <li data-bbox="698 861 1989 901">■ 48 V DC in (via 3-pin terminal block); 12 V, 5 A minimum out

11.2 Firmware Specifications

The following tables summarize the switch's firmware features.

Port Control

Table 11-5: Port Control

FEATURE	DESCRIPTION
Port speed, duplex mode, flow ctrl	
Port frame size	Jumbo frames
Port state	Administrative status
Port status	Link monitoring
Port Statistics	MIB counters
Port VeriPHY	Cable diagnostics
Dual media TP/SFP auto-detection	

Table 11-6: Port Control

FEATURE	DESCRIPTION
Port speed, duplex mode, flow ctrl	
Port frame size	Jumbo frames
Port state	Administrative status
Port status	Link monitoring
Port Statistics	MIB counters
Port VeriPHY	Cable diagnostics
Dual media TP/SFP auto-detection	

QoS

Table 11-7: QoS

FEATURE	DESCRIPTION
Traffic classes	8 active priorities
Port default priority	
User priority	
Input priority mapping	

Table 11-7: QoS

FEATURE	DESCRIPTION
Scheduler mode	
QoS Control List	QCL Mode
Storm control	Unicast, Multicast and Broadcast
Port policers	
Global/VCAP (ACL) policers	
Port egress shaper	
Queue egress shapers	
DiffServ (RFC2474) re-marking	
Tag re-marking	
QoS (WRED)	

L2 Switching

Table 11-8: L2 Switching

FEATURE	DESCRIPTION
IEEE 802.1D bridge	Automatic MAC address learning / aging Static MAC addresses

Table 11-8: L2 Switching

FEATURE	DESCRIPTION
IEEE 802.1Q	Virtual LAN Static Private VLAN Static port isolation MAC-based VLAN Protocol-based VLAN Generic Attribute Registration Protocol (GARP) GARP VLAN Registration Protocol (GVRP) Multiple Registration Protocol (MRP) Multiple VLAN Registration Protocol (MVRP)
IEEE 802.1ad provider bridge	Native or translated VLAN
IEEE 802.1Q-2005	Multiple Spanning Tree Protocol: MSTP, RSTP and STP Rapid Spanning Tree Protocol: RSTP and STP
MRSTP	Up to 12 instances (without trunking) RSTP/MRSTP port set as non-edge port automatically if STP port configured RSTP/MRSTP loop detection
IEEE 802.3ad	Link Aggregation Control Protocol (LACP) Static link aggregation
BPDU	Guard and restricted role Transparency

Table 11-8: L2 Switching

FEATURE	DESCRIPTION
IGMP v2/v3	Snooping, throttling, filtering and leave proxy
MLD	Snooping, throttling, filtering and leave proxy
MVR	
Voice VLAN	
DHCP	Client Snooping Option 82 relay
DHCP v6	Client
DNS	Client, proxy
ARP	Inspection
Port mirroring	
Protection	1+1 port protection 1:1 port protection
G.8032 ring protection v1/v2 (XGS3600-26F only)	Up to 12 instances
IP MAC binding	

Security and Synchronization

Table 11-9: Security and Synchronization

FEATURE	DESCRIPTION
Network Access Server (NAS)	Port-based 802.1x Single 802.1x Multiple 802.1x MAC-based authentication VLAN assignment QoS assignment Guest VLAN
RADIUS	Accounting, authentication and accounting
MAC address limit	
TACACS+	Accounting, authentication and accounting
Web & CLI	authentication
Authorization	15 user levels
ACL	Filtering, policing, port copy
IP source guard	
Remote Switched Port Analyzer (RSPAN)	

Table 11-9: Security and Synchronization

FEATURE	DESCRIPTION
Dying gasp	
SYNCHRONIZATION	
SNTP client	
NTPv4 client	

OAM

Table 11-10: OAM

FEATURE	DESCRIPTION
IEEE 802.3ah link OAM	Variable, request, response Discovery process, information, event notification and loopback
Flow OAM	Ingress and egress
IEEE 802.1ag Connectivity Fault Management (CFM)	Fault Management (FM): <ul style="list-style-type: none"> ■ continuity check & remote defect indication (ETH-CC + ETH-RDI) ■ loopback (ETH-LB) ■ link trace (ETH-LT)

Table 11-10: OAM

FEATURE	DESCRIPTION
ITU-T recommendation Y.1731	<p>Vitesse OAM Y.1731 PHY solution</p> <p>MEP:</p> <ul style="list-style-type: none"> ■ FM: automatic protection switching (ETH-APS + ETH-RAPS) ■ EPS/ERPS using ETH-CCM <p>MIP:</p> <ul style="list-style-type: none"> ■ FM: link trace PDU (LTM) respond ■ FM: loop back PDU (LBM) respond

Robustness and Power Saving

Table 11-11: Robustness and Power Saving

FEATURE	DESCRIPTION
Cold start	
Warm start	
POWER SAVING	
ActivePHY	
PerfectReach	

Table 11-11: Robustness and Power Saving

FEATURE	DESCRIPTION
IEEE 802.3az Energy Efficient Ethernet (EEE)	
Thermal protection	

Management

Table 11-12: Management

FEATURE	DESCRIPTION
HTTP server	
CLI	All parameters are configurable via console port & telnet
Management access filtering	
HTTPS	
SSH v2	
IPv6 management	
System syslog	
Software update via web	
SNMP v1/v2/v3 agent	

Table 11-12: Management

FEATURE	DESCRIPTION
IEEE 802.1AB Link Layer Discovery Protocol (LLDP)	
TIA 1057 LLDP-MED	
Cisco Discovery Protocol (CDP)	
sFlow	
Configuration download/upload	
Dual image	

MIBs

Table 11-13: MIBs

FEATURE	DESCRIPTION
RFC 2674 VLAN MIB	
IEEE 802.1Q bridge MIB 2008	
RFC 1213 MIB II	
RFC 1215 TRAPS MIB	

Table 11-13: MIBs

FEATURE	DESCRIPTION
RFC 4188 Bridge MIB	
RFC 5519 Multicast Group Membership Discovery MIB	
RFC 4668 RADIUS auth. Client MIB	
RFC 4670 RADIUS Accounting MIB	
RFC 3635 Ethernet-like MIB	
RFC 2863 Interface Group MIB using SMI v2	
RFC 3636 802.30 MAU MIB	
RFC 4133 Entity MIB version 3	
RFC 3411 SNMP Management Frameworks	
RFC 3414 User-based Security Model for SNMPv3	
RFC 3415 View-based access Control Model for SNMP	
IEEE 802.1 MSTP MIB	

Table 11-13: MIBs

FEATURE	DESCRIPTION
IEEE 802.1AB LLDP-MIB (LLDP MIB included in a clause of the STD)	
IEEE 802.30ad (LACP MIB included in a clause of the STD)	
IEEE 802.1X (PAE MIB included in a clause of the STD)	
TIA 1057 LLDP-MED (MIB is part of the STD)	
Private MIB framework	
ZyXEL private MIB	For every function

11.3 EMI/Safety Specifications

The following table summarizes the switch's EMI/safety specifications.

Table 11-14: EMI/Safety Specifications

ITEM	DESCRIPTION	REMARK
Safety	BSMI	
EMI	BSMI	
RoHS	Level A	

Table 11-14: EMI/Safety Specifications

ITEM	DESCRIPTION	REMARK
Reliability Test Reports	MTBF of Prediction Report	Telcordia SR-332 issue 2 (100,000 hrs at least)
	Free Fall (Drop) Test Report	ISTA Project 2A
	Random Vibration Test Report	IEC-60068-2-64
	Storage Test Report	Temperature: -40 ~ 70°C Humidity: 10 ~ 95% R.H Test duration: 72 hours
	Operation Cold (low temperature) Test	
	Operation Dry Heat (High temperature) Test	
	Operation Temperature Cycles Test	
	E-cap Lifetime Test	43800 hours
	Thermal Shock Test	
	Damp Heat Steady State Test	
	Thermal Profile Test	
	ESD Simulation Test report	
	High/Low Temperature Start Test	

Table 11-14: EMI/Safety Specifications

ITEM	DESCRIPTION	REMARK
Environmental specifications	2002/95/EC (RoHS) Restriction of Hazardous Substances Directive 2002/96/EC (WEEE) (WEEE) Waste Electrical and Electronic Equipment Directive European Parliament and Council Directive 94/62/EC of 20 December 1994 on packaging and packaging waste	

Part IV: Front Matter

Appendix A

A.1 Glossary of Web Based Management

A

ACE

ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID.

ACL

ACL is an acronym for Access Control List. It is the list of ACEs that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier for its ACL. The privileges determine whether there are specific traffic object access rights. ACL implementations can be complex, for example, when the ACEs are prioritized. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

AES

AES (Advanced Encryption Standard) is a U.S. government encryption standard which replaces DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. AES is used as the encryption key protocol in the 802.11i standard to improve WLAN security.

Aggregation

Aggregation is the use of multiple ports in parallel to increase the link speed beyond the limits of a single port and to increase redundancy for higher availability.

ARP

ARP (Address Resolution Protocol) is used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the IP address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the IP address of the desired destination system.

ARP Inspection

ARP Inspection is a security feature. Several types of attacks can be launched against a host or devices connected to Layer-2 networks by poisoning the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C**CC**

CC (Continuity Check) is a MEP function that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

CCM

CCM (Continuity Check Message) is an OAM frame transmitted from a MEP to its peer MEP that is used to implement CC functionality.

CDP

CDP is an acronym for Cisco Discovery Protocol.

D

DEI

DEI (Drop Eligible Indicator) is a 1-bit field in the VLAN tag.

DES

DES (Data Encryption Standard) provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded data. Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP

DHCP (Dynamic Host Configuration Protocol) is used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server. The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between clients and the server when they are not on the same subnet.

The DHCP option 82 enables a DHCP relay agent to insert specific information into DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The Circuit ID is 4 bytes in length and its format is {vlan_id}{module_id}{port_no}. The vlan_id is the first two bytes. The module_id is the third byte (in standalone switches it always equal 0, in stackable switches it means switch ID). The port_no is the fourth byte.

The Remote ID is 6 bytes in length, and is equal to the DHCP relay agent's MAC address.

DHCP Snooping

DHCP Snooping is used to prevent attackers from adding their own DHCP servers to the network.

DNS

DNS (Domain Name System) stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into IP addresses. For example, the domain name `www.example.com` might translate to `192.168.0.1`.

DoS

DoS (Denial of Service) is a kind of network attack that attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connections, an attacker may be able to prevent network users from accessing services (e.g. email, web etc.) that rely on the affected computer.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets. An IPv4 dotted decimal address has the form `x.y.z.w`, where `x`, `y`, `z` and `w` are decimal numbers between 0 and 255.

DSCH

DSCH (Differentiated Services Code Point) is a field in the header of IP packets for packet classification purposes.

E

EEE

EEE is an abbreviation for Energy Efficient Ethernet as defined in IEEE 802.3az.

EPS

EPS (Ethernet Protection Switching), more recently known as Ethernet Linear Protection Switching provides redundancy for point-to-point links as defined in ITU/T G.8031.

Ethernet Type

Ethernet Type or EtherType is a field in the Ethernet MAC header. It is used to indicate which protocol is being transported in an Ethernet frame.

F

FTP

FTP (File Transfer Protocol) provides file writing, reading, directory and security services over TCP.

Fast Leave

Multicast snooping fast leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

H

HTTP

HTTP (Hypertext Transfer Protocol) conveys information on the World Wide Web (WWW). HTTP defines how messages are formatted and transmitted, and what actions Web servers and clients should take in response to various commands.

The Web browser (HTTP client) uses HTTP to send requests to servers. A HTTP client initiates a request by establishing a TCP connection to a particular port on a remote host (port 80 by default). A HTTP server listening on that port waits for the client to send a request message and responds to them when they arrive.

HTTPS

HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer) secures HTTP connections by providing authentication and encrypted communication. HTTPS is really just the use of Secure Sockets Layer (SSL) as a sublayer under its regular HTTP (HTTPS uses port 443 instead of HTTP port 80 in its interactions with TCP). SSL uses a 128-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

ICMP (Internet Control Message Protocol) is used to convey error responses or generate diagnostics. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IMAP

IMAP (Internet Message Access Protocol) is used by email clients to retrieve email messages from a mail server. IMAP has several advantages over another popular mail retrieval protocol, Post Office Protocol version 3 (POP3). IMAP enables multiple access to each mailbox, retrieval of any MIME part of an email and server-side searches.

IP

IP (Internet Protocol) is provides a logical IP addressing scheme for hosts and routes packets between them via the network layer. IP enables packets to cross interconnected networks so these networks appear as a single logical network at the network or IP layer. Each device directly connected to the Internet must have a unique IP address. IP is a best-effort system, which means that no packet is assured to reach its destination in the same condition it was sent.

IPv4 (IP version 4) uses 32 bits to represent over four billion unique addresses. IPv4 addresses are becoming depleted because of the increasing number of devices directly connected to the Internet and because they were allocated in blocks, the bulk of which remain unused. IPv6 (IP version 6) solves this problem by providing the same service using 128 bits to represent over 3×10^{38} addresses. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IPMC means IP Multicast.

IP Source Guard

IP Source Guard is used to prevent attackers from spoofing their IP addresses by dropping packets that don't have source IP addresses allocated via DHCP or configured manually in the DHCP Snooping table.

L

LACP

LACP (Link Aggregation Control Protocol) is an IEEE 802.3ad standard protocol that allows bundling several physical ports together to form a single logical port.

LLC

The IEEE 802.2 Logical Link Control (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (e.g. IP and IPX) to coexist within a multipoint network. The LLC header consists of a 1-byte DSAP (Destination Service Access Point), a 1-byte SSAP (Source Service Access Point), a 1 or 2-byte Control field followed by LLC information or the payload from a higher level protocol.

LLDP

The Link Layer Discovery Protocol (LLDP) specified in the IEEE 802.1ab standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LOC

LOC is an acronym for Loss Of Connectivity and is detected by a MEP and is indicating lost connectivity in the network. LOC can be used as a switch criteria by EPS.

M

MAC Table

The MAC Table is a table of ports and source MAC addresses that is initially empty. It is often implemented as Content Addressable Memory (CAM). When the first frame arrives on a port, the port number and source MAC address is added to the MAC Table. When a new frame arrives, its destination MAC address is looked up in the MAC Table to find the destination port to send the frame to. After a preconfigured time, entries time-out and are removed from the MAC Table. This is dynamic updating, but the MAC Table can also be updated manually using static entries that are never removed.

MEP

MEP is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5

MD5 is an acronym for Message-Digest algorithm 5. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

MLD is an acronym for Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.

The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them (Wikipedia).

N

NAS

NAS is an acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS

NetBIOS is an acronym for Network Basic Input/Output System. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS

NFS is an acronym for Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP

NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

O

OAM

OAM is an acronym for Operation Administration and Maintenance.

It is a protocol described in ITU-T Y.1731 used to implement carrier ethernet functionality. MEP functionality like CC and RDI is based on this Optional TLVs.

A LLDP frame contains multiple TLVs

For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled the corresponding information is not included in the LLDP frame.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

P

PCP

PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that implement the Ethernet physical layer (IEEE-802.3).

PING

ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

POP3

POP3 is an acronym for Post Office Protocol version 3. It is a protocol for email clients to retrieve email messages from a mail server.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a store-and-forward service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

Private VLAN

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

PTP

PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.

Q

QCE

QCE is an acronym for QoS Control Entry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: Low, Normal, Medium, and High for individual application.

QCL

QCL is an acronym for QoS Control List. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

R

RARP

RARP is an acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS is an acronym for Remote Authentication Dial In User Service. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RDI

RDI is an acronym for Remote Defect Indication. It is a OAM functionality that is used by a MEP to indicate defect detected to the remote peer MEP.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

SHA

SHA is an acronym for Secure Hash Algorithm. It is designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP

SMTP is an acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP

The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP

SNMP is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allows diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SPROUT

Stack Protocol using ROUting Technology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform shortest path forwarding within the stack.

SSID

Service Set Identifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (wikipedia).

SSH

SSH is an acronym for Secure SHell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM

SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP

Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

Switch ID

Switch IDs (1-16) are used to uniquely identify the switches within a stack. The Switch ID of each switch is shown on the display on the front of the switch and is used widely in the web pages as well as in the CLI commands.

SyncE

SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

T

TACACS+

TACACS+ is an acronym for Terminal Access Controller Access Control System Plus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP

TCP is an acronym for Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for TELetype NETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP

TFTP is an acronym for Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

U

UDP

UDP is an acronym for User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

V

VLAN

Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

Appendix B

B.1 Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site. The following columns are shown.

- **Name:** This is a short, descriptive name for the service.
- **Protocol:** This is the type of IP protocol used by the service. If this is TCP/UDP, then the service uses the same port number with TCP and UDP. If this is User-Defined, the Port(s) is the IP protocol number, not the port number.
- **Port(s):** This value depends on the Protocol. Please refer to RFC 1700 for further information about port numbers.
 - If the Protocol is TCP, UDP or TCP/UDP this is the IP port number.
 - If the Protocol is User-Defined, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table B-1: Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.

Table B-1: Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648, 24032	A popular video conferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20, 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/ server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.

Table B-1: Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.

Table B-1: Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).

Appendix C

C.1 Legal Information

Copyright

Copyright © 2012 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning

This device has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CLASS 1 LASER PRODUCT

APPAREIL A LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.
PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Viewing Certifications

1. Go to <http://www.zyxel.com>.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

INDEX

A

AAA 8-25
Activate Alternate Image 9-4
Admin Edge 7-34, 7-44
Admin P2P 7-44
Admin State 8-17
Aggr ID 7-26
Aging Period 8-16, 8-33
Allow Guest VLAN if EAPOL Seen 8-17
APS MEP 7-138
Architecture 7-137
ARP SMAC Match 7-18
ARP/RARP and Request/Reply 7-17
Authentication Method 8-45
Authentication Password 6-25, 6-32
Authentication Protocol 6-25, 6-32
Auto Configuration 6-19
Auto Edge 7-34
Automatic Redirect 8-44

B

Baud Rate 7-10
BIOS Version 6-6
BPDU Guard 7-35
Bridge FDB Size 6-7
Bridge ID 7-37

Bridge Instance 7-37
Bridge Priority 7-30

C

CDP Aware 7-62
Chassis ID 7-64
CIST Role 7-39
CIST State 7-39
Classified DP Level 7-104
Clock Source 6-11
Community 6-24
Configured Link Speed 7-3
Connector Type 7-10
Console Baudrate 6-7
Contact 6-6
Current Link Speed 7-3
Custom S-ports 7-80

D

Datagram Size 7-118
Date Code 7-11
Daylight Savings 6-11
Daylight Savings Type 6-11
Dead Time 8-25
Default DEI 7-104
Default PCP 7-104

DEI 7-97, 7-105, 7-111
Dest. Port Filter 7-19
Device Name 6-6
DHCP Client 6-17
DIP Filter 7-19
Discovery State 7-128
DMAC Filter 7-16
DMAC Type 7-111
DNS 6-18
DNS Proxy 6-18
DNS Server 6-18
Domain 7-135
DP Bypass Level 7-99
DP Level 7-105
DP level 7-98, 7-105
DPL 7-107, 7-113
DPort 7-113
DSAP Address 7-112
DSCP 7-70, 7-107, 7-113
DSCP Based 7-97

E

EAPOL Counters 8-23
EAPOL Timeout 8-15
Edge Port BPDU Filtering 7-31
Edge Port BPDU Guard 7-31
Egress Remap 7-108
Egress Rule 7-80
Engine ID 6-23
EPRS ID 7-139
EPS ID 7-137

EtherType Filter 7-17, 7-111
Excessive Collision Mode 7-4

F

Fallback 8-45
Fallback to Local Authorization 8-26
Fan Speed 6-8
Fast Leave 7-49
Fiber Type 7-10
Filtering Groups 7-52
Firmware Version 6-7
Flash Size 6-7
Flooding 7-99
Flow Control 7-3, 7-100
Forward Delay 7-30
Frame Type 7-16
FW-Delay 7-42

G

GARP/MRP Applicant 7-91
Gateway 6-19
Gateway IP Address 6-7
Group Name 6-16, 6-27, 6-29, 7-122
Guest VLAN Enabled 8-16, 8-20
Guest VLAN ID 8-17
GVRP/MVRP Mode 7-93
GVRP/MVRP rrole 7-94

H

Hardware-Mechanical Version 6-7
Hash Code Contributors 7-23
Hello-Time 7-42
Hold Time 8-16
Host IP Address 6-7
Host MAC Address 6-7

I

ICMP Code Filter 7-19
ICMP Flooding Enabled 7-48
ICMP Type Filter 7-19
IGMP or MLD Querier 7-50
Immediate Leave 7-58
Inband Default Gateway 6-18
Inband IP Address or Outband IP Address 6-17
Inband IP Gateway or Outband IP Gateway 6-17
Inband IP Mask or Outband IP Mask 6-17
Inband VLAN ID 6-17
Ingress Classify 7-106, 7-108
Ingress Filtering 7-80
Ingress Translate 7-106, 7-108
Internal Root Cost 7-37
IP Address 6-19
IP Fragment 7-19
IP Option 7-19
IP Protocol Filter 7-18
IP TTL 7-19
IP/Ethernet Length 7-18

L

LACP Key 7-25
LACP Received 7-28
LACP Role 7-25
LACP Transmitted 7-28
Last Authentication 8-24
Last ID 8-22
Learning 7-99
Link Monitor support 7-125
Link Monitoring Support 7-128
LLDP-MED Capabilities 7-72
LLQI 7-51
Local Time 6-11
Location 6-6
Log Level 6-21
Logging 7-13
Loopback Operation 7-125
Loopback support 7-125

M

Mail Server 7-123
Major Ring ID 7-140
Max Age 7-30
Max Dynamic Clients 8-3
Max Hdr Size 7-120
Max. Reauth. Count 8-17
Max-Age 7-42
Maximum Frame Size 6-7, 7-4
Maximum Hop Count 7-30
MIB Retrieval Support 7-125

7-128

Migrate Check 7-45
Model Name 6-6
MTU Size 7-129
Multiplexer State 7-129
MVR Mode 7-57

O

OAM Enabled 7-124
OAM Mode 7-124
OID Subtree 6-28

P

P flow 7-137
P SF MEP 7-138
Parser State 7-129
Partner Key 7-26
Partner System ID 7-26
Password 6-14
Path Cost 7-34, 7-36, 7-38
PCP 7-97, 7-105
PDU Permission 7-128
PDU Revision 7-129
Period Threshold 7-127
Policer 7-99
Policy Filter 7-16
Policy ID 7-12
Polling Interval 7-120
Port Copy 7-13, 7-20
Port Error Recovery 7-31

Port Error Recovery Timeout 7-31
Power Control 7-4
Powers 6-8
Prefix 6-19
Privacy Password 6-26, 6-32
Privacy Protocol 6-26, 6-32
Privilege Level 6-14
Privilege Levels 6-16
Proxy Enabled 7-49
PVID 7-81, 7-83

Q

QI 7-50
QoS Class 7-107, 7-109
QoS class 7-97, 7-105
QRI 7-51

R

RADIUS-Assigned QoS Enabled 8-16, 8-19
RADIUS-Assigned VLAN Enabled 8-16, 8-19
RAM Size 6-7
RARP DMAC Match 7-18
Rate Limiter 7-20
Rate Limiter ID 7-12, 7-14
Read View Name 6-30
Reauthentication Period 8-15
Receiver Id 7-118
Regional Root 7-37
Relay Information Mode 8-12
Relay Information Policy 8-12

Relay Mode 8-12
 Relay Server 8-12
 Remote Loopback Support 7-128
 Remote Port ID 7-64
 Residence Port 7-135
 Resolve Conflict 7-115
 Restricted Role 7-35
 Restricted TCN 7-35
 Return-Path 7-123
 Ring Type 7-139
 Root Cost 7-37
 Root ID 7-37
 Root Port 7-37
 Router Port 7-49
 Rv 7-50
 RxPacket Threshold 7-127

S

Sampling Rate 7-120
 Scheduler Mode 7-102
 Security Level 6-25, 6-29, 6-31
 Security Model 6-27, 6-29
 Security Name 6-27, 6-31
 Sender IP Filter and Target IP Filter 7-17
 Serial Number 6-7
 Server IP 6-31
 Server Mode 6-20
 Severity Level 6-31, 7-122
 sFlow Instance 7-120
 sFlow Port 7-120
 Shutdown 7-13

SIP Filter 7-19
 SMAC 7-111
 SMAC Filter 7-16
 SNMP State 6-23
 Snooping Enabled 7-48, 7-50
 Source IP 6-24
 Source Mask 6-24
 Source Port Filter 7-19
 SPort 7-113
 SSAP Address 7-112
 SSM Range 7-49
 STP Enabled 7-34
 Subnet Mask 6-7
 Syslog Level 6-20
 System Capabilities 7-64
 System Contact 6-9
 System Date 6-6
 System Description 6-6
 System Location 6-9
 System Name 6-9
 System Uptime 6-6

T

Tag Class 7-97
 Tag Classification 7-97
 Tag Priority 7-17
 Tag Remarking Mode 7-104
 TCP ACK 7-20
 TCP FIN 7-20
 TCP PSH 7-20
 TCP RST 7-20

TCP SYN 7-20
TCP URG 7-20
TELNET 8-41
Temperature 1 to 4 6-8
Throttling 7-49
Time Set Offset 6-11
Time Zone Offset 6-11
Topology Change Count 7-38
Topology Change Last 7-38
Topology Flag 7-37
Transmit Hold Count 7-31
Transmit Queue 6-7
Trap Version 6-31
Tx Central Wavelength 7-10

U

UDP Port 6-31
Unidirectional Operation Support 7-128
URI 7-51
User Module Name 8-36
User Name 6-14, 6-24, 6-25

V

Vcc 7-11
Vendor Name 7-10
Vendor OUI 7-10
Vendor P/N 7-10
Vendor Rev 7-10
Vendor SN 7-10
View Name 6-28

View Type 6-28
Virtual Channel 7-140
VLAN ID Filter 7-16
VLAN User 7-82

W

W flow 7-137
W SF MEP 7-137
Window 7-127
Write View Name 6-30